

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001169

International filing date: 21 January 2005 (21.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-044141
Filing date: 20 February 2004 (20.02.2004)

Date of receipt at the International Bureau: 10 March 2005 (10.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

21.01.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 2 月 2 0 日
Date of Application:

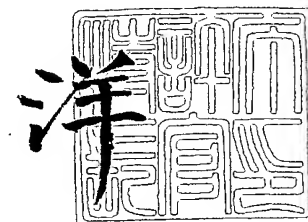
出 願 番 号 特 願 2 0 0 4 - 0 4 4 1 4 1
Application Number:
[ST. 10/C] : [J P 2 0 0 4 - 0 4 4 1 4 1]

出 願 人 松 下 電 器 産 業 株 式 有 限 公 司
Applicant(s):

2 0 0 5 年 2 月 2 5 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2054051229
【提出日】 平成16年 2月20日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 29/06
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 吉田 順二
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 ▲浜▼井 信二
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 松見 知代子
【特許出願人】
 【識別番号】 000005821
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100086405
 【弁理士】
 【氏名又は名称】 河宮 治
 【電話番号】 06-6949-1261
 【ファクシミリ番号】 06-6949-0361
【選任した代理人】
 【識別番号】 100098280
 【弁理士】
 【氏名又は名称】 石野 正弘
 【電話番号】 06-6949-1261
 【ファクシミリ番号】 06-6949-0361
【手数料の表示】
 【予納台帳番号】 163028
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 0318000

【書類名】特許請求の範囲**【請求項 1】**

ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムにおいて設けられ、上記要求発行機器から上記要求受諾機器への接続要求信号を転送するサーバ装置において

、上記複数の機器にそれぞれ関連付けられた IP アドレス及びポート番号、並びに上記各機器の機器 ID からなる上記各機器に係る機器情報の組を含む機器情報リストを格納するための機器情報格納手段を備え、

上記要求受諾機器に係る機器情報の組を含みかつ上記要求受諾機器から定期的に送信される機器登録信号を受信し、上記受信された機器登録信号に含まれる上記要求受諾機器に係る機器情報の組を上記機器情報格納手段に格納し、

上記要求発行機器から送信される第 1 の TCP 接続開始信号を受信することにより上記要求発行機器との間の第 1 の TCP 接続を確立し、

上記要求受諾機器の機器 ID と、上記要求発行機器に関連付けられた IP アドレス及びポート番号とを含む上記要求受諾機器への第 1 の接続要求信号を上記第 1 の TCP 接続を用いて上記要求発行機器から受信し、

上記受信された第 1 の接続要求信号に含まれる上記要求受諾機器の機器 ID を上記機器情報リストから検索し、上記機器情報リスト上で、上記第 1 の接続要求信号に含まれる要求受諾機器の機器 ID と一致した機器 ID を含む機器情報の組に係る機器を上記要求受諾機器として識別し、上記機器情報リスト上で、上記識別された要求受諾機器に係る機器情報の組に含まれる IP アドレス及びポート番号を上記要求受諾機器に関連付けられた IP アドレス及びポート番号として識別し、

上記識別された要求受諾機器に対して、上記識別された IP アドレス及びポート番号を宛先として、上記受信された第 1 の接続要求信号に含まれる上記要求発行機器に関連付けられた IP アドレス及びポート番号を含む第 2 の接続要求信号を、上記機器登録信号に対する応答信号として送信することを特徴とするサーバ装置。

【請求項 2】

上記サーバ装置は、

上記識別された要求受諾機器に係る機器情報の組に含まれる IP アドレス及びポート番号を上記要求受諾機器に関連付けられた IP アドレス及びポート番号として識別した後であって、かつ上記識別された要求受諾機器に上記第 2 の接続要求信号を送信する前に、上記要求受諾機器に第 3 の接続要求信号を送信し、上記第 3 の接続要求信号に対する応答信号として第 2 の TCP 接続開始信号を上記要求受諾機器から受信することにより上記要求受諾機器との間において第 2 の TCP 接続を確立し、

上記確立された第 2 の TCP 接続を用いて上記要求受諾機器に上記第 2 の接続要求信号を送信することを特徴とする請求項 1 記載のサーバ装置。

【請求項 3】

上記第 1 の接続要求信号は、上記要求受諾機器のパスワード情報をさらに含み、

上記サーバ装置は、上記第 1 の接続要求信号に含まれた上記パスワード情報を上記第 2 の接続要求信号に付加して送信することを特徴とする請求項 2 記載のサーバ装置。

【請求項 4】

上記サーバ装置は、

送受信する信号を暗号化しかつ復号化するための第 1 及び第 2 の通信用共通鍵を生成し、上記第 1 の通信用共通鍵を用いて受信する信号の復号化を実行し、上記第 2 の通信用共通鍵を用いて送信する信号の暗号化を実行する第 1 の暗号通信手段と、上記サーバ装置の正当性を証明するためのサーバ証明書情報を格納した証明書情報格納手段とを備え、

上記第 1 の接続要求信号を受信する前に、上記要求発行機器に上記サーバ証明書情報を送信し、

上記要求発行機器から、上記サーバ証明書情報に応答して生成された第 1 の共通鍵作成

情報を上記第 1 の T C P 接続を用いて受信し、上記第 1 の共通鍵作成情報に応答して上記第 1 の暗号通信手段により第 2 の共通鍵作成情報を生成し、上記第 1 の共通鍵作成情報及び上記第 2 の共通鍵作成情報に基づいて上記第 1 の暗号通信手段により第 1 の通信用共通鍵を生成する一方、上記第 2 の共通鍵作成情報を上記要求発行機器に上記第 1 の T C P 接続を用いて送信し、上記第 1 の通信用共通鍵と同一の通信用共通鍵を上記第 1 の共通鍵作成情報及び上記第 2 の共通鍵作成情報に基づいて上記要求発行機器に生成させることにより上記第 1 の通信用共通鍵を上記要求発行機器との間で共有し、

上記要求発行機器から、上記第 1 の通信用共通鍵を用いて暗号化された上記第 1 の接続要求信号を、上記第 1 の T C P 接続を用いて受信し、上記受信された第 1 の接続要求信号を、上記第 1 の通信用共通鍵を用いて上記第 1 の暗号通信手段により復号化し、

上記第 2 の接続要求信号を送信する前に、上記要求受諾機器に上記サーバ証明書情報を送信し、

上記要求受諾機器から、上記サーバ証明書情報に응答して生成された第 3 の共通鍵作成情報を上記第 2 の T C P 接続を用いて受信し、上記第 3 の共通鍵作成情報に응答して上記第 1 の暗号通信手段により第 4 の共通鍵作成情報を生成し、上記第 3 の共通鍵作成情報及び上記第 4 の共通鍵作成情報に基づいて上記第 1 の暗号通信手段により第 2 の通信用共通鍵を生成する一方、上記第 4 の共通鍵作成情報を上記要求受諾機器に上記第 2 の T C P 接続を用いて送信し、上記第 2 の通信用共通鍵と同一の通信用共通鍵を上記第 3 の共通鍵作成情報及び上記第 4 の共通鍵作成情報に基づいて上記要求受諾機器に生成させることにより上記第 2 の通信用共通鍵を上記要求受諾機器との間で共有し、

上記第 1 の接続要求信号を受信した後であってかつ上記第 2 の接続要求信号を送信する前に、上記第 2 の通信用共通鍵を用いて上記第 1 の暗号通信手段により上記第 2 の接続要求信号を暗号化することを特徴とする請求項 3 記載のサーバ装置。

【請求項 5】

ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムにおいて設けられ、上記サーバ装置及び上記要求受諾機器と通信する要求発行機器において、

上記サーバ装置に第 1 の T C P 接続開始信号を送信することによって上記サーバ装置との間の第 1 の T C P 接続を確立し、

上記要求受諾機器の機器 I D と上記要求発行機器に関連付けられた I P アドレス及びポート番号とを含む上記要求受諾機器への第 1 の接続要求信号を上記サーバ装置に上記第 1 の T C P 接続を用いて送信し、

上記要求発行機器と上記要求受諾機器との間の通信を要求する通信要求信号を上記要求受諾機器から受信した後に、上記通信要求信号に응答して上記要求発行機器と上記要求受諾機器との間の通信を受諾し、上記要求受諾機器との通信を開始することを特徴とする要求発行機器。

【請求項 6】

上記第 1 の接続要求信号は、上記要求受諾機器のパスワード情報をさらに含むことを特徴とする請求項 5 記載の要求発行機器。

【請求項 7】

上記要求発行機器は、

送受信する信号を暗号化しかつ復号化するための第 1 の通信用共通鍵を生成し、上記第 1 の通信用共通鍵を用いて送信する信号の暗号化を実行する第 2 の暗号通信手段と、上記サーバ装置の正当性を証明するためのサーバ証明書情報を認証する第 1 の証明書情報認証手段とを備え、

上記第 1 の接続要求信号を送信する前に、上記サーバ装置から上記サーバ証明書情報を受信し、

上記受信されたサーバ証明書情報を上記第 1 の証明書情報認証手段により認証し、上記受信されたサーバ証明書情報が正規であるか否かを確認し、

上記受信されたサーバ証明書情報を正規であると確認したとき、上記第 2 の暗号通信手

段により第1の共通鍵作成情報を生成し、上記生成された第1の共通鍵作成情報を上記第1のTCP接続を用いて上記サーバ装置に送信し、上記サーバ装置から、上記第1の共通鍵作成情報に回答して生成された第2の共通鍵作成情報を上記第1のTCP接続を用いて受信し、上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記第2の暗号通信手段により第1の通信用共通鍵を生成する一方、上記第1の通信用共通鍵と同一の通信用共通鍵を上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記サーバ装置に生成させることにより上記第1の通信用共通鍵を上記サーバ装置との間で共有し、

上記第1の接続要求信号を送信する前に、上記第1の通信用共通鍵を用いて上記第2の暗号通信手段により上記第1の接続要求信号を暗号化し、

上記暗号化された上記第1の接続要求信号を上記第1のTCP接続を用いて上記サーバ装置に送信することを特徴とする請求項6記載の要求発行機器。

【請求項8】

ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムにおいて設けられ、上記サーバ装置及び上記要求発行機器と通信する要求受諾機器であって、

上記要求受諾機器の機器IDを格納した機器ID格納手段を備え、

上記要求受諾機器の機器IDを含む機器登録信号を上記サーバ装置に定期的に送信し、

上記要求発行機器に関連付けられたIPアドレス及びポート番号を含む第2の接続要求信号を、上記機器登録信号に対する応答信号として上記サーバ装置から受信し、

上記受信された第2の接続要求信号に含まれたIPアドレス及びポート番号が表す上記要求発行機器に、上記要求受諾機器と上記要求発行機器との間の通信を要求する通信要求信号を送信し、

上記要求発行機器が上記通信要求信号に回答して上記要求受諾機器と上記要求発行機器との間の通信を受諾した後に、上記要求発行機器との通信を開始することを特徴とする要求受諾機器。

【請求項9】

上記要求受諾機器は、

上記機器登録信号を上記サーバ装置に送信した後であって上記第2の接続要求信号を受信する前に、上記機器登録信号に対する応答信号として上記サーバ装置から第3の接続要求信号を受信し、上記第3の接続要求信号に対する応答信号として第2のTCP接続開始信号を上記サーバ装置に送信することにより上記サーバ装置との間において第2のTCP接続を確立し、

上記確立された第2のTCP接続を用いて上記サーバ装置から上記第2の接続要求信号を受信することを特徴とする請求項8記載の要求受諾機器。

【請求項10】

上記要求受諾機器は、

上記要求受諾機器のパスワード情報を格納したパスワード情報格納手段を備え、

パスワード情報をさらに含む上記第2の接続要求信号を、上記第2のTCP接続を用いて上記サーバ装置から受信し、

上記第2の接続要求信号に含まれたパスワード情報が、上記パスワード情報格納手段に格納された上記要求受諾機器のパスワード情報と一致している場合にのみ、上記要求発行機器に上記通信要求信号を送信することを特徴とする請求項9記載の要求受諾機器。

【請求項11】

上記要求受諾機器は、

送受信する信号を暗号化しかつ復号化するための第2の通信用共通鍵を生成し、上記第2の通信用共通鍵を用いて受信する信号の復号化を実行する第3の暗号通信手段と、上記サーバ装置の正当性を証明するためのサーバ証明書情報を認証する第2の証明書情報認証手段とを備え、

上記第2の接続要求信号を受信する前に、上記サーバ装置から上記サーバ証明書情報を

受信し、

上記受信されたサーバ証明書情報を上記第2の証明書情報認証手段により認証し、上記受信されたサーバ証明書情報が正規であるか否かを確認し、

上記受信されたサーバ証明書情報を正規であると確認したとき、上記第3の暗号通信手段により第3の共通鍵作成情報を生成し、上記生成された第3の共通鍵作成情報を上記第2のTCP接続を用いて上記サーバ装置に送信し、上記サーバ装置から、上記第3の共通鍵作成情報に応答して生成された第4の共通鍵作成情報を上記第2のTCP接続を用いて受信し、上記第2の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記第3の暗号通信手段により第2の通信用共通鍵を生成する一方、上記第2の通信用共通鍵と同一の通信用共通鍵を上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記サーバ装置に生成させることにより上記第2の通信用共通鍵を上記サーバ装置との間で共有し、

上記サーバ装置から、上記第2の通信用共通鍵を用いて暗号化された上記第2の接続要求信号を、上記第2のTCP接続を用いて受信し、上記受信された第2の接続要求信号を、上記第2の通信用共通鍵を用いて上記第3の暗号通信手段により復号化することの特徴とする請求項10記載の要求受諾機器。

【請求項12】

請求項1記載のサーバ装置と、請求項5記載の要求発行機器及び請求項8記載の要求受諾機器を含む複数の機器とを備えた通信システムであって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続されたことを特徴とする通信システム。

【請求項13】

請求項2記載のサーバ装置と、請求項5記載の要求発行機器及び請求項9記載の要求受諾機器を含む複数の機器とを備えた通信システムであって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続されたことを特徴とする通信システム。

【請求項14】

請求項3記載のサーバ装置と、請求項6記載の要求発行機器及び請求項10記載の要求受諾機器を含む複数の機器とを備えた通信システムであって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続されたことを特徴とする通信システム。

【請求項15】

請求項4記載のサーバ装置と、請求項7記載の要求発行機器及び請求項11記載の要求受諾機器を含む複数の機器とを備えた通信システムであって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続されたことを特徴とする通信システム。

【請求項16】

ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムに設けられ、上記要求発行機器から上記要求受諾機器への接続要求信号を転送するサーバ装置を用いた通信方法において、上記サーバ装置は、上記複数の機器にそれぞれ関連付けられたIPアドレス及びポート番号、並びに上記各機器の機器IDからなる上記各機器に係る機器情報の組を含む機器情報リストを格納するための機器情報格納手段を備え、

上記通信方法は、

上記要求受諾機器に係る機器情報の組を含みかつ上記要求受諾機器から定期的に送信される機器登録信号を受信し、上記受信された機器登録信号に含まれる上記要求受諾機器に係る機器情報の組を上記機器情報格納手段に格納するステップと、

上記要求発行機器から送信される第1のTCP接続開始信号を受信することにより上記要求発行機器との間の第1のTCP接続を確立するステップと、

上記要求受諾機器の機器IDと、上記要求発行機器に関連付けられたIPアドレス及び

ポート番号とを含む上記要求受諾機器への第1の接続要求信号を上記第1のTCP接続を用いて上記要求発行機器から受信するステップと、

上記受信された第1の接続要求信号に含まれる上記要求受諾機器の機器IDを上記機器情報リストから検索し、上記機器情報リスト上で、上記第1の接続要求信号に含まれる要求受諾機器の機器IDと一致した機器IDを含む機器情報の組に係る機器を上記要求受諾機器として識別し、上記機器情報リスト上で、上記識別された要求受諾機器に係る機器情報の組に含まれるIPアドレス及びポート番号を上記要求受諾機器に関連付けられたIPアドレス及びポート番号として識別するステップと、

上記識別された要求受諾機器に対して、上記識別されたIPアドレス及びポート番号を宛先として、上記受信された第1の接続要求信号に含まれる上記要求発行機器に関連付けられたIPアドレス及びポート番号を含む第2の接続要求信号を、上記機器登録信号に対する応答信号として送信するステップとを含むことを特徴とする通信方法。

【請求項17】

上記識別するステップの後であって上記第2の接続要求信号を送信するステップの前に、上記要求受諾機器に第3の接続要求信号を送信し、上記第3の接続要求信号に対する応答信号として第2のTCP接続開始信号を上記要求受諾機器から受信することにより上記要求受諾機器との間において第2のTCP接続を確立するステップをさらに含み、

上記第2の接続要求信号を送信するステップは、上記確立された第2のTCP接続を用いて上記要求受諾機器に上記第2の接続要求信号を送信することを特徴とする請求項16記載の通信方法。

【請求項18】

上記第1の接続要求信号は、上記要求受諾機器のパスワード情報をさらに含み、

上記通信方法は、上記第1の接続要求信号に含まれた上記パスワード情報を上記第2の接続要求信号に付加して送信するステップをさらに含むことを特徴とする請求項17記載の通信方法。

【請求項19】

上記通信方法は、

上記第1の接続要求信号を受信するステップの前に、上記サーバ装置の正当性を証明するためのサーバ証明書情報を上記要求発行機器に送信するステップと、

上記要求発行機器から、上記サーバ証明書情報に応答して生成された第1の共通鍵作成情報を上記第1のTCP接続を用いて受信し、上記第1の共通鍵作成情報に応答して第2の共通鍵作成情報を生成し、上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて第1の通信用共通鍵を生成する一方、上記第2の共通鍵作成情報を上記要求発行機器に上記第1のTCP接続を用いて送信し、上記第1の通信用共通鍵と同一の通信用共通鍵を上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記要求発行機器に生成させることにより上記第1の通信用共通鍵を上記要求発行機器との間で共有するステップと、

上記要求発行機器から、上記第1の通信用共通鍵を用いて暗号化された上記第1の接続要求信号を、上記第1のTCP接続を用いて受信し、上記受信された第1の接続要求信号を、上記第1の通信用共通鍵を用いて復号化するステップと、

上記第2の接続要求信号を送信するステップの前に、上記要求受諾機器に上記サーバ証明書情報を送信するステップと、

上記要求受諾機器から、上記サーバ証明書情報に応答して生成された第3の共通鍵作成情報を上記第2のTCP接続を用いて受信し、上記第3の共通鍵作成情報に応答して第4の共通鍵作成情報を生成し、上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて第2の通信用共通鍵を生成する一方、上記第4の共通鍵作成情報を上記要求受諾機器に上記第2のTCP接続を用いて送信し、上記第2の通信用共通鍵と同一の通信用共通鍵を上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記要求受諾機器に生成させることにより上記第2の通信用共通鍵を上記要求受諾機器との間で共有するステップと、

上記第1の接続要求信号を受信するステップの後であってかつ上記第2の接続要求信号を送信するステップの前に、上記第2の通信用共通鍵を用いて上記第2の接続要求信号を暗号化するステップとをさらに含むことを特徴とする請求項18記載の通信方法。

【請求項20】

ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムに設けられ、上記サーバ装置及び上記要求受諾機器と通信する要求発行機器を用いた通信方法において、

上記サーバ装置に第1のTCP接続開始信号を送信することによって上記サーバ装置との間の第1のTCP接続を確立するステップと、

上記要求受諾機器の機器IDと上記要求発行機器に関連付けられたIPアドレス及びポート番号とを含む上記要求受諾機器への第1の接続要求信号を上記サーバ装置に上記第1のTCP接続を用いて送信するステップと、

上記要求発行機器と上記要求受諾機器との間の通信を要求する通信要求信号を上記要求受諾機器から受信した後に、上記通信要求信号に回答して上記要求発行機器と上記要求受諾機器との間の通信を受諾し、上記要求受諾機器との通信を開始するステップとを含むことを特徴とする通信方法。

【請求項21】

上記第1の接続要求信号は、上記要求受諾機器のパスワード情報をさらに含むことを特徴とする請求項20記載の通信方法。

【請求項22】

上記通信方法は、

上記第1の接続要求信号を送信するステップの前に、上記サーバ装置から上記サーバ証明書情報を受信するステップと、

上記受信されたサーバ証明書情報を認証し、上記受信されたサーバ証明書情報が正規であるか否かを確認するステップと、

上記受信されたサーバ証明書情報を正規であると確認したとき、第1の共通鍵作成情報を生成し、上記生成された第1の共通鍵作成情報を上記第1のTCP接続を用いて上記サーバ装置に送信し、上記サーバ装置から、上記第1の共通鍵作成情報に回答して生成された第2の共通鍵作成情報を上記第1のTCP接続を用いて受信し、上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて第1の通信用共通鍵を生成する一方、上記第1の通信用共通鍵と同一の通信用共通鍵を上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記サーバ装置に生成させることにより上記第1の通信用共通鍵を上記サーバ装置との間で共有するステップと、

上記第1の接続要求信号を送信するステップの前に、上記第1の通信用共通鍵を用いて上記第1の接続要求信号を暗号化するステップとをさらに含むことを特徴とする請求項21記載の通信方法。

【請求項23】

ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムに設けられ、上記サーバ装置及び上記要求発行機器と通信する要求受諾機器を用いた通信方法であって、

上記要求受諾機器の機器IDを含む機器登録信号を上記サーバ装置に定期的に送信するステップと、

上記要求発行機器に関連付けられたIPアドレス及びポート番号を含む第2の接続要求信号を、上記機器登録信号に対する応答信号として上記サーバ装置から受信するステップと、

上記受信された第2の接続要求信号に含まれたIPアドレス及びポート番号が表す上記要求発行機器に、上記要求受諾機器と上記要求発行機器との間の通信を要求する通信要求信号を送信するステップと、

上記要求発行機器が上記通信要求信号に回答して上記要求受諾機器と上記要求発行機器との間の通信を受諾した後に、上記要求発行機器との通信を開始するステップとを含むこ

とを特徴とする通信方法。

【請求項 2 4】

上記機器登録信号を上記サーバ装置に送信するステップの後であって上記第 2 の接続要求信号を受信するステップの前に、上記機器登録信号に対する応答信号として上記サーバ装置から第 3 の接続要求信号を受信し、上記第 3 の接続要求信号に対する応答信号として第 2 の T C P 接続開始信号を上記サーバ装置に送信することにより上記サーバ装置との間において第 2 の T C P 接続を確立するステップと、

上記確立された第 2 の T C P 接続を用いて上記サーバ装置から上記第 2 の接続要求信号を受信するステップとをさらに含むことを特徴とする請求項 2 3 記載の通信方法。

【請求項 2 5】

上記要求受諾機器は、上記要求受諾機器のパスワード情報を格納したパスワード情報格納手段を備え、

上記第 2 の接続要求信号はパスワード情報をさらに含み、

上記第 2 の接続要求信号に含まれたパスワード情報が、上記パスワード情報格納手段に格納された上記要求受諾機器のパスワード情報と一致している場合にのみ、上記要求発行機器に上記通信要求信号を送信することを特徴とする請求項 2 4 記載の通信方法。

【請求項 2 6】

上記通信方法は、

上記第 2 の接続要求信号を受信するステップの前に、上記サーバ装置から上記サーバ証明書情報を受信するステップと、

上記受信されたサーバ証明書情報を認証し、上記受信されたサーバ証明書情報が正規であるか否かを確認するステップと、

上記受信されたサーバ証明書情報を正規であると確認したとき、第 3 の共通鍵作成情報を生成し、上記生成された第 3 の共通鍵作成情報を上記第 2 の T C P 接続を用いて上記サーバ装置に送信し、上記サーバ装置から、上記第 3 の共通鍵作成情報に応答して生成された第 4 の共通鍵作成情報を上記第 2 の T C P 接続を用いて受信し、上記第 2 の共通鍵作成情報及び上記第 4 の共通鍵作成情報に基づいて第 2 の通信用共通鍵を生成する一方、上記第 2 の通信用共通鍵と同一の通信用共通鍵を上記第 3 の共通鍵作成情報及び上記第 4 の共通鍵作成情報に基づいて上記サーバ装置に生成させることにより上記第 2 の通信用共通鍵を上記サーバ装置との間で共有するステップとをさらに含み、

上記第 2 の接続要求信号を受信するステップは、上記受信された第 2 の接続要求信号を、上記第 2 の通信用共通鍵を用いて復号化するステップをさらに含むことを特徴とする請求項 2 5 記載の通信方法。

【請求項 2 7】

上記サーバ装置と、上記要求発行機器及び上記要求受諾機器を含む複数の機器とを備えた通信システムを用いた通信方法であって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続され、

請求項 1 6 記載の通信方法に係る各ステップと、請求項 2 0 記載の通信方法に係る各ステップと、請求項 2 3 記載の通信方法に係る各ステップとを含むことを特徴とする通信方法。

【請求項 2 8】

上記サーバ装置と、上記要求発行機器及び上記要求受諾機器を含む複数の機器とを備えた通信システムを用いた通信方法であって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続され、

請求項 1 7 記載の通信方法に係る各ステップと、請求項 2 0 記載の通信方法に係る各ステップと、請求項 2 4 記載の通信方法に係る各ステップとを含むことを特徴とする通信方法。

【請求項 2 9】

上記サーバ装置と、上記要求発行機器及び上記要求受諾機器を含む複数の機器とを備えた通信システムを用いた通信方法であって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続され、
請求項 1 8 記載の通信方法に係る各ステップと、請求項 2 1 記載の通信方法に係る各ステップと、請求項 2 5 記載の通信方法に係る各ステップとを含むことを特徴とする通信方法。

【請求項 3 0】

上記サーバ装置と、上記要求発行機器及び上記要求受諾機器を含む複数の機器とを備えた通信システムを用いた通信方法であって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続され、
請求項 1 9 記載の通信方法に係る各ステップと、請求項 2 2 記載の通信方法に係る各ステップと、請求項 2 6 記載の通信方法に係る各ステップとを含むことを特徴とする通信方法。

【請求項 3 1】

請求項 1 6 乃至 1 9 のうちの 1 つの通信方法に係る各ステップを含むことを特徴とするプログラム。

【請求項 3 2】

請求項 2 0 乃至 2 2 のうちの 1 つの通信方法に係る各ステップを含むことを特徴とするプログラム。

【請求項 3 3】

請求項 2 3 乃至 2 6 のうちの 1 つの通信方法に係る各ステップを含むことを特徴とするプログラム。

【請求項 3 4】

請求項 2 7 乃至 3 0 のうちの 1 つの通信方法に係る各ステップを含むことを特徴とするプログラム。

【書類名】明細書

【発明の名称】サーバ装置、要求発行機器、要求受諾機器、通信システム及び通信方法

【技術分野】

【0001】

本発明は、TCP/IPプロトコル群を用いた通信システムであり、例えばインターネット等のネットワークに接続された機器間においてピアツーピア接続による通信を行うためのサーバ装置と、接続要求信号を発行する要求発行機器と、接続要求信号を受諾する要求受諾機器と、サーバ装置、要求発行機器及び要求受諾機器を含む通信システムと、通信方法とに関する。本発明はさらに、上記通信方法に係る各ステップを含むプログラムに関する。

【背景技術】

【0002】

近年、xDSLや光ファイバケーブルなどのブロードバンド環境が整ったことにより、企業、一般家庭を問わずインターネットが急速に普及してきている。また、パーソナルコンピュータ（PC）だけでなく、テレビジョン受像機やDVDレコーダなどのAV機器や、エアコンディショナー、冷蔵庫のような白物家庭電気製品もインターネットに接続できるようになってきている。本願明細書では、上記インターネットなどのネットワークに接続されて通信を行う機器を、「通信機器」又は「機器」という。

【0003】

家庭や企業内のローカルエリアネットワーク（以下、LANという。）からインターネットに接続する場合には、ネットワーク・アドレス変換（Network Address Translation；以下、NATという。）機能やネットワーク・アドレス・ポート変換（Network Address Port Translation；以下、NAPTという。）機能を有するルータ装置を用いるのが一般的になっている。

【0004】

インターネットに接続された機器間において通信を行う場合には、機器毎に一意に割り当てられたグローバルIPアドレスが使用される。しかし、インターネットに接続する機器の急増により、グローバルIPアドレスの数が不足する傾向にある。そのため、インターネットに直接接続されないLANにおいては、RFC1918により規定されたLAN内においてのみ一意であるプライベートIPアドレスが使用されることが多い。ただし、プライベートIPアドレスはインターネット上においては一意ではなく、またその使用を許されていないため、プライベートIPアドレスを有する機器は、そのままではインターネットに接続された他の機器との通信ができない。

【0005】

NATもしくはNAPT機能は、こうした問題を解決するもので、プライベートIPアドレスとグローバルIPアドレスの相互変換を行い、LAN上においてプライベートIPアドレスが割り当てられた機器が、インターネット上の機器と通信を行えるようにする。

【0006】

以下、NAPT機能の仕組みについて、図10乃至図12を用いて説明する。

【0007】

図10は、従来技術の通信システムのネットワーク構成の一例を示すブロック図である。図10において、要求受諾機器13とNAPT機能を有するルータ装置104とはLAN106を構成し、LAN106は、ルータ装置104のWAN側のポートにおいてインターネット（WAN）105に接続されている。サーバ装置11と、要求発行機器12もまた、インターネット（WAN）105に接続されている。

【0008】

ここでは、いわゆるインターネットをLANとを明確に区別するために、インターネットをWAN（Wide Area Network）と表記することにする。

【0009】

図11は、NAPT機能を用いた通信の通信シーケンス図の一例である。図11におい

て、パケット21は、要求受諾機器13からルータ装置104に送信されるパケットであり、パケット23は、ルータ104においてパケット21に対して往路変換処理のステップS22を実行することにより、ルータ装置104からサーバ装置11に送信されるパケットである。同様に、パケット25は、サーバ装置11からルータ装置104に送信されるパケットであり、パケット27は、ルータ装置104においてパケット25に対して復路変換処理のステップS26を実行することにより、ルータ装置104から要求受諾機器13に送信されるパケットである。また、図12は、ルータ装置104のNAPTテーブルの一例を示す表であり、ルータ装置104内のテーブルメモリ（図示せず。）には、このNAPTテーブルの内容が記憶されている。

【0010】

ここで、図10に示されたように、サーバ装置11にはグローバルIPアドレス“130.74.23.6”が割り当てられ、ルータ装置104のWAN側にはグローバルIPアドレス“202.204.16.13”が割り当てられており、また要求受諾機器13にはプライベートIPアドレス“192.168.1.3”が割り当てられているものとする。

【0011】

インターネット上における通信に用いられるIPパケットには、送信元（ソース）を特定する発信元IPアドレスフィールド（以下、SAという。）と、宛先（ディステーション）を指定する宛先IPアドレスフィールド（以下、DAという。）が含まれている。また通信プロトコルとして、TCP（Transmission Control Protocol）やUDP（User Datagram Protocol）を使用する場合には、IPパケットにさらに送信元（ソース）のポート番号である発信元ポート番号フィールド（以下、SPという。）と宛先（ディステーション）のポート番号である宛先ポート番号フィールド（以下、DPという。）が含まれる。

【0012】

要求受諾機器13が、サーバ装置11とTCP通信する場合には、例えば図11のようなパケット21をルータ装置104に送信する。パケット21には、発信元を特定するSA“192.168.1.3”及びSP“2000”と、宛先を示すDA“130.743.23.6”及びDP“1200”とが含まれている。

【0013】

ルータ装置104は、受信したパケット21に往路変換処理のステップS22を実行し、処理後のパケット23を、宛先であるサーバ装置11に送信する。往路変換処理のステップS22において、ルータ装置104は、プライベートIPアドレスであるSA“192.168.1.3”を、ルータ装置104のWAN側グローバルIPアドレスである“202.204.16.13”に置換し、同時にSP“2000”をルータ装置104のWAN側ポート番号“3400”に置換する。このとき、ルータ装置104は、図12のように、IPアドレス“192.168.1.3”及び“202.204.16.13”とポート番号“2000”及び“3400”との組を、NAPTテーブルに保存しておく。

【0014】

さて、サーバ装置11はパケット23を受信すると、所定の応答処理のステップS24を行った後、パケット23に対する応答として、パケット25をルータ装置104に送信する。パケット25には、発信元を特定するSA“130.743.23.6”及びSP“1200”と、宛先を示すDA“202.204.16.13”及びDP“3400”とが含まれている。

【0015】

ルータ装置104は、パケット25を受信すると、NAPTテーブルを参照し、パケット25に復路変換処理のステップS26を実行し、処理後のパケット27を要求受諾機器13に送信する。復路変換処理のステップS26において、ルータ装置104は、まずNAPTテーブルからDA“202.204.16.13”とDP“3400”の組を参照

する。ここではこの組は存在しているので、ルータ装置 104 は、パケット 25 上の DA を “202. 204. 16. 13” から “192. 168. 1. 3” に置換し、パケット 25 上の DP を “3400” から “2000” に置換する。

【0016】

NAPT テーブル内のデータは、その通信が行われている間中は保持され、通信が終了すると破棄される。

【0017】

以上の動作により、LAN 内のプライベート IP アドレスを持つ機器からインターネット上の機器への通信を行うことができる。ただし、この場合だと、反対にインターネット上の機器から LAN 内のプライベート IP アドレスを持つ機器への通信を開始することができない。

【0018】

そこでこれを解決するために、静的 NAPT と呼ばれる機能がある。すなわち、予め静的な NAPT テーブルをルータ装置 104 上に設定しておく。静的な NAPT テーブルの内容は、図 12 の NAPT テーブルと同様であるが、この場合 WAN 側のポート番号は、設定時に未使用のポート番号を指定しなければならない。静的 NAPT 機能を用いると、例えばインターネット側の機器から、設定されたグローバル IP アドレスとポート番号に対してパケットを送信すると、ルータ装置 104 が図 11 と同様に IP アドレスとポート番号の変換を行うことにより、LAN 上のプライベート IP アドレスを持つ要求受諾機器 13 にパケットが到達することになる。これにより、インターネット上の機器から LAN 内のプライベート IP アドレスを持つ機器への通信を行えるようになる。

【0019】

ところで、ルータ装置 104 のグローバル IP アドレスは常に一定であるとは限らない。例えば、PPP (Point-to-Point Protocol) を用いてインターネットサービスプロバイダと接続し、又は DHCP (Dynamic Host Configuration Protocol) により IP アドレスが動的に割り当てられる場合には、インターネットに接続する毎にグローバル IP アドレスが変わることがある。このため、接続先機器のグローバル IP アドレスを把握しておくのは困難となる。また静的 NAPT を用いていると、通信していない間も LAN 上の機器へのアクセスが可能となるため、セキュリティが低くなってしまう。

【0020】

こうした課題を解決するための通信システムが、特許文献 1 において提案されており、以下、図 10 乃至図 13 を用いて、特許文献 1 において提案されている通信システムについて説明する。

【0021】

図 13 は、図 10 の通信システムの通信シーケンスの一例を示すシーケンス図である。ここで、図 10 に示されたように、要求発行機器 12 には、グローバル IP アドレスとして “8. 117. 12. 109” が割り当てられているものとする。また要求受諾機器 13 は、一意に割り当てられた機器 ID を内部のメモリ (図示せず。) に格納しているものとする。

【0022】

要求受諾機器 13 は、定期的に、機器 ID をペイロードに持つ機器登録パケット 31 を、UDP を用いてサーバ装置 11 に送信する。UDP パケットである機器登録パケット 31 の SA には、要求受諾機器 13 のプライベート IP アドレスである “192. 168. 1. 3” が書き込まれているが、機器登録パケット 31 がルータ装置 104 を通るときに、上記説明したように NAPT 機能によって機器登録パケット 31 の SA と SP が変換され、サーバ装置 11 に送信される。サーバ装置 11 は、受信した機器登録パケット 31 を参照し、ステップ S32 において要求受諾機器 13 の機器 ID、グローバル IP アドレス及びポート番号の組を保存しておく。

【0023】

要求受諾機器 13 は、定期的に機器登録パケット 31 をサーバ装置 11 に送信するため

、ルータ装置 104 のグローバル IP アドレスもしくは WAN 側ポート番号が変更になった場合でも、ステップ S32 や、同様のステップ S32A などが実行されることにより、サーバ装置 11 に保存された要求受諾機器 13 の機器 ID、グローバル IP アドレス及びポート番号の組は自動的に更新される。

【0024】

一方、要求発行機器 12 が要求受諾機器 13 との通信を行いたい場合には、要求発行機器 12 は、まずサーバ装置 11 に TCP 接続開始パケット 33 を送信することによってサーバ装置 11 との TCP 接続を確立し、接続相手である要求受諾機器 13 の機器 ID を書き込んだ接続要求パケット 34 をサーバ装置 11 に送信する。サーバ装置 11 は、接続要求パケット 34 を受信すると、ステップ S35 において、内部のメモリ（図示せず。）に可能している機器 ID のリストを参照し、接続要求パケット 34 内に含まれた機器 ID の情報と同じ機器 ID の情報が存在すれば、この機器 ID に関連付けられている IP アドレス及びポート番号が示す機器に対して、UDP を用いて接続要求通知パケット 36 を送信する。接続要求通知パケット 36 は、機器登録パケット 31 に対する応答としてルータ装置 104 に送信されるため、ルータ装置 104 において IP アドレスとポート番号の変換が行われ、要求受諾機器 13 に到達できる。要求受諾機器 13 は、接続要求通知パケット 36 を受信すると、サーバ装置 11 に対して TCP 接続開始パケット 37 を送信することによってサーバ装置 11 との TCP 接続を確立する。

【0025】

以降、要求発行機器 12 が、TCP 接続開始パケット 33 により開始された TCP 接続を用いてコマンド信号 38 をサーバ装置 11 に送信すると、サーバ装置 11 は、TCP 接続開始パケット 37 により開始された TCP 接続を用いてコマンド信号 38 を要求受諾機器 13 に転送できるようになる。同様に、要求受諾機器 13 が、TCP 接続開始パケット 37 により開始された TCP 接続を用いてサーバ装置 11 にパケットを送信すると、サーバ装置 11 は、TCP 接続開始パケット 33 により開始された TCP 接続を用いてこのパケットを要求発行機器 12 に転送する。

【0026】

以上のようにして、サーバ装置 11 を中継することにより、インターネット上のグローバル IP アドレスを持つ機器である要求発行機器 12 と、プライベート IP アドレスを持つ LAN 上の機器である要求受諾機器 13 との間において、通信を行うことができるようになる。要求発行機器 12 が別の LAN 上に存在し、ルータ装置を通してインターネットに接続されている場合でも、同様の動作により要求受諾機器 13 との通信を行える。

【0027】

また、特許文献 2 では、互いのグローバル IP アドレスを知らないインターネット上の機器間において直接伝送を行う、すなわちピアツーピア伝送を行うための情報処理システムが開示されている。グローバル IP アドレスを有するクライアント間であるパーソナルコンピュータ同士の接続をピアツーピア接続とし、その他のクライアント間の接続をサーバを経由したクライアント・サーバ型接続とさせる。ピアツーピア接続はサーバから取得した互いのグローバル IP アドレスに基づいて確立され、クライアント・サーバ型接続からピアツーピア型接続への一部遷移によって、サーバに対するトラフィックの一局集中を避けることができる。

【0028】

【特許文献 1】特許 3445986 号公報。

【特許文献 2】特開 2003-203023 号公報。

【発明の開示】

【発明が解決しようとする課題】

【0029】

上記説明した特許文献 1 記載の通信システムは、常にサーバ装置 11 経由により通信を行うため、例えば機器間において動画データのように大容量のデータを伝送しようとする、サーバ装置 11 に多大な負荷がかかるという問題があった。特に複数組の通信が同時

に行われると、複数台のサーバ装置により分散処理を行っても対応できない可能性もある。

【0030】

また、特許文献2記載の情報処理システムは、グローバルIPアドレスを持つ機器同士でのみピアツーピア伝送を行うようになっており、プライベートIPアドレスを持つLAN上の機器の場合はピアツーピア伝送を行わないようになっている。

【0031】

本発明の目的は以上の問題点を解決し、プライベートIPアドレスをそれぞれ持つ異なるLAN上の機器間においてピアツーピア伝送を実現し、かつ不正アクセスを許さないサーバ装置、要求発行機器、要求受諾機器、通信システム及び通信方法を提供することにある。また、本発明の別の目的は、上記通信方法に係る各ステップを含むプログラムを提供することにある。

【課題を解決するための手段】

【0032】

本発明の第1の態様に係るサーバ装置は、ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムにおいて設けられ、上記要求発行機器から上記要求受諾機器への接続要求信号を転送し、

上記サーバ装置は、

上記複数の機器にそれぞれ関連付けられたIPアドレス及びポート番号、並びに上記各機器の機器IDからなる上記各機器に係る機器情報の組を含む機器情報リストを格納するための機器情報格納手段を備え、

上記要求受諾機器に係る機器情報の組を含みかつ上記要求受諾機器から定期的に送信される機器登録信号を受信し、上記受信された機器登録信号に含まれる上記要求受諾機器に係る機器情報の組を上記機器情報格納手段に格納し、

上記要求発行機器から送信される第1のTCP接続開始信号を受信することにより上記要求発行機器との間の第1のTCP接続を確立し、

上記要求受諾機器の機器IDと、上記要求発行機器に関連付けられたIPアドレス及びポート番号とを含む上記要求受諾機器への第1の接続要求信号を上記第1のTCP接続を用いて上記要求発行機器から受信し、

上記受信された第1の接続要求信号に含まれる上記要求受諾機器の機器IDを上記機器情報リストから検索し、上記機器情報リスト上で、上記第1の接続要求信号に含まれる要求受諾機器の機器IDと一致した機器IDを含む機器情報の組に係る機器を上記要求受諾機器として識別し、上記機器情報リスト上で、上記識別された要求受諾機器に係る機器情報の組に含まれるIPアドレス及びポート番号を上記要求受諾機器に関連付けられたIPアドレス及びポート番号として識別し、

上記識別された要求受諾機器に対して、上記識別されたIPアドレス及びポート番号を宛先として、上記受信された第1の接続要求信号に含まれる上記要求発行機器に関連付けられたIPアドレス及びポート番号を含む第2の接続要求信号を、上記機器登録信号に対する応答信号として送信することを特徴とする。

【0033】

また、上記サーバ装置は、

上記識別された要求受諾機器に係る機器情報の組に含まれるIPアドレス及びポート番号を上記要求受諾機器に関連付けられたIPアドレス及びポート番号として識別した後であって、かつ上記識別された要求受諾機器に上記第2の接続要求信号を送信する前に、上記要求受諾機器に第3の接続要求信号を送信し、上記第3の接続要求信号に対する応答信号として第2のTCP接続開始信号を上記要求受諾機器から受信することにより上記要求受諾機器との間において第2のTCP接続を確立し、

上記確立された第2のTCP接続を用いて上記要求受諾機器に上記第2の接続要求信号を送信することを特徴とする。

【0034】

さらに、上記サーバ装置において、
上記第1の接続要求信号は、上記要求受諾機器のパスワード情報をさらに含み、
上記サーバ装置は、上記第1の接続要求信号に含まれた上記パスワード情報を上記第2の接続要求信号に付加して送信することを特徴とする。

【0035】

またさらに、上記サーバ装置は、
送受信する信号を暗号化しかつ復号化するための第1及び第2の通信用共通鍵を生成し、
上記第1の通信用共通鍵を用いて受信する信号の復号化を実行し、上記第2の通信用共通鍵を用いて送信する信号の暗号化を実行する第1の暗号通信手段と、上記サーバ装置の正当性を証明するためのサーバ証明書情報を格納した証明書情報格納手段とを備え、

上記第1の接続要求信号を受信する前に、上記要求発行機器に上記サーバ証明書情報を送信し、

上記要求発行機器から、上記サーバ証明書情報に応答して生成された第1の共通鍵作成情報を上記第1のTCP接続を用いて受信し、上記第1の共通鍵作成情報に応答して上記第1の暗号通信手段により第2の共通鍵作成情報を生成し、上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記第1の暗号通信手段により第1の通信用共通鍵を生成する一方、上記第2の共通鍵作成情報を上記要求発行機器に上記第1のTCP接続を用いて送信し、上記第1の通信用共通鍵と同一の通信用共通鍵を上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記要求発行機器に生成させることにより上記第1の通信用共通鍵を上記要求発行機器との間で共有し、

上記要求発行機器から、上記第1の通信用共通鍵を用いて暗号化された上記第1の接続要求信号を、上記第1のTCP接続を用いて受信し、上記受信された第1の接続要求信号を、上記第1の通信用共通鍵を用いて上記第1の暗号通信手段により復号化し、

上記第2の接続要求信号を送信する前に、上記要求受諾機器に上記サーバ証明書情報を送信し、

上記要求受諾機器から、上記サーバ証明書情報に応答して生成された第3の共通鍵作成情報を上記第2のTCP接続を用いて受信し、上記第3の共通鍵作成情報に応答して上記第1の暗号通信手段により第4の共通鍵作成情報を生成し、上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記第1の暗号通信手段により第2の通信用共通鍵を生成する一方、上記第4の共通鍵作成情報を上記要求受諾機器に上記第2のTCP接続を用いて送信し、上記第2の通信用共通鍵と同一の通信用共通鍵を上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記要求受諾機器に生成させることにより上記第2の通信用共通鍵を上記要求受諾機器との間で共有し、

上記第1の接続要求信号を受信した後であってかつ上記第2の接続要求信号を送信する前に、上記第2の通信用共通鍵を用いて上記第1の暗号通信手段により上記第2の接続要求信号を暗号化することを特徴とする。

【0036】

本発明の第2の態様に係る要求発行機器は、ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムにおいて設けられ、上記サーバ装置及び上記要求受諾機器と通信し、

上記要求発行機器は、

上記サーバ装置に第1のTCP接続開始信号を送信することによって上記サーバ装置との間の第1のTCP接続を確立し、

上記要求受諾機器の機器IDと上記要求発行機器に関連付けられたIPアドレス及びポート番号とを含む上記要求受諾機器への第1の接続要求信号を上記サーバ装置に上記第1のTCP接続を用いて送信し、

上記要求発行機器と上記要求受諾機器との間の通信を要求する通信要求信号を上記要求受諾機器から受信した後に、上記通信要求信号に応答して上記要求発行機器と上記要求受

諸機器との間の通信を受諾し、上記要求受諾機器との通信を開始することを特徴とする。

【0037】

また、上記要求発行機器において、上記第1の接続要求信号は、上記要求受諾機器のパスワード情報をさらに含むことを特徴とする。

【0038】

さらに、上記要求発行機器は、

送受信する信号を暗号化しかつ復号化するための第1の通信用共通鍵を生成し、上記第1の通信用共通鍵を用いて送信する信号の暗号化を実行する第2の暗号通信手段と、上記サーバ装置の正当性を証明するためのサーバ証明書情報を認証する第1の証明書情報認証手段とを備え、

上記第1の接続要求信号を送信する前に、上記サーバ装置から上記サーバ証明書情報を受信し、

上記受信されたサーバ証明書情報を上記第1の証明書情報認証手段により認証し、上記受信されたサーバ証明書情報が正規であるか否かを確認し、

上記受信されたサーバ証明書情報を正規であると確認したとき、上記第2の暗号通信手段により第1の共通鍵作成情報を生成し、上記生成された第1の共通鍵作成情報を上記第1のTCP接続を用いて上記サーバ装置に送信し、上記サーバ装置から、上記第1の共通鍵作成情報に応答して生成された第2の共通鍵作成情報を上記第1のTCP接続を用いて受信し、上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記第2の暗号通信手段により第1の通信用共通鍵を生成する一方、上記第1の通信用共通鍵と同一の通信用共通鍵を上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記サーバ装置に生成させることにより上記第1の通信用共通鍵を上記サーバ装置との間で共有し、

上記第1の接続要求信号を送信する前に、上記第1の通信用共通鍵を用いて上記第2の暗号通信手段により上記第1の接続要求信号を暗号化し、

上記暗号化された上記第1の接続要求信号を上記第1のTCP接続を用いて上記サーバ装置に送信することを特徴とする。

【0039】

本発明の第3の態様に係る要求受諾機器は、ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムにおいて設けられ、上記サーバ装置及び上記要求発行機器と通信し、

上記要求受諾機器は、

上記要求受諾機器の機器IDを格納した機器ID格納手段を備え、

上記要求受諾機器の機器IDを含む機器登録信号を上記サーバ装置に定期的に送信し、

上記要求発行機器に関連付けられたIPアドレス及びポート番号を含む第2の接続要求信号を、上記機器登録信号に対する応答信号として上記サーバ装置から受信し、

上記受信された第2の接続要求信号に含まれたIPアドレス及びポート番号が表す上記要求発行機器に、上記要求受諾機器と上記要求発行機器との間の通信を要求する通信要求信号を送信し、

上記要求発行機器が上記通信要求信号に응答して上記要求受諾機器と上記要求発行機器との間の通信を受諾した後に、上記要求発行機器との通信を開始することを特徴とする。

【0040】

また、上記要求受諾機器は、

上記機器登録信号を上記サーバ装置に送信した後であって上記第2の接続要求信号を受信する前に、上記機器登録信号に対する応答信号として上記サーバ装置から第3の接続要求信号を受信し、上記第3の接続要求信号に対する応答信号として第2のTCP接続開始信号を上記サーバ装置に送信することにより上記サーバ装置との間において第2のTCP接続を確立し、

上記確立された第2のTCP接続を用いて上記サーバ装置から上記第2の接続要求信号

を受信することを特徴とする。

【0041】

さらに、上記要求受諾機器は、

上記要求受諾機器のパスワード情報を格納したパスワード情報格納手段を備え、パスワード情報をさらに含む上記第2の接続要求信号を、上記第2のTCP接続を用いて上記サーバ装置から受信し、

上記第2の接続要求信号に含まれたパスワード情報が、上記パスワード情報格納手段に格納された上記要求受諾機器のパスワード情報と一致している場合にのみ、上記要求発行機器に上記通信要求信号を送信することを特徴とする。

【0042】

またさらに、上記要求受諾機器は、

送受信する信号を暗号化しかつ復号化するための第2の通信用共通鍵を生成し、上記第2の通信用共通鍵を用いて受信する信号の復号化を実行する第3の暗号通信手段と、上記サーバ装置の正当性を証明するためのサーバ証明書情報を認証する第2の証明書情報認証手段とを備え、

上記第2の接続要求信号を受信する前に、上記サーバ装置から上記サーバ証明書情報を受信し、

上記受信されたサーバ証明書情報を上記第2の証明書情報認証手段により認証し、上記受信されたサーバ証明書情報が正規であるか否かを確認し、

上記受信されたサーバ証明書情報を正規であると確認したとき、上記第3の暗号通信手段により第3の共通鍵作成情報を生成し、上記生成された第3の共通鍵作成情報を上記第2のTCP接続を用いて上記サーバ装置に送信し、上記サーバ装置から、上記第3の共通鍵作成情報に応答して生成された第4の共通鍵作成情報を上記第2のTCP接続を用いて受信し、上記第2の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記第3の暗号通信手段により第2の通信用共通鍵を生成する一方、上記第2の通信用共通鍵と同一の通信用共通鍵を上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記サーバ装置に生成させることにより上記第2の通信用共通鍵を上記サーバ装置との間で共有し、

上記サーバ装置から、上記第2の通信用共通鍵を用いて暗号化された上記第2の接続要求信号を、上記第2のTCP接続を用いて受信し、上記受信された第2の接続要求信号を、上記第2の通信用共通鍵を用いて上記第3の暗号通信手段により復号化することを特徴とする。

【0043】

本発明の第4の態様に係る通信システムは、本発明に係る第1の態様のサーバ装置と、本発明に係る第2の態様の要求発行機器及び本発明に係る第3の態様の要求受諾機器を含む複数の機器とを備え、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続されたことを特徴とする。

【0044】

本発明の第5の態様に係る通信方法は、ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムに設けられ、上記要求発行機器から上記要求受諾機器への接続要求信号を転送するサーバ装置を用いた通信方法であって、上記サーバ装置は、上記複数の機器にそれぞれ関連付けられたIPアドレス及びポート番号、並びに上記各機器の機器IDからなる上記各機器に係る機器情報の組を含む機器情報リストを格納するための機器情報格納手段を備え、

上記通信方法は、

上記要求受諾機器に係る機器情報の組を含みかつ上記要求受諾機器から定期的に送信される機器登録信号を受信し、上記受信された機器登録信号に含まれる上記要求受諾機器に係る機器情報の組を上記機器情報格納手段に格納するステップと、

上記要求発行機器から送信される第1のTCP接続開始信号を受信することにより上記要求発行機器との間の第1のTCP接続を確立するステップと、

上記要求受諾機器の機器IDと、上記要求発行機器に関連付けられたIPアドレス及びポート番号とを含む上記要求受諾機器への第1の接続要求信号を上記第1のTCP接続を用いて上記要求発行機器から受信するステップと、

上記受信された第1の接続要求信号に含まれる上記要求受諾機器の機器IDを上記機器情報リストから検索し、上記機器情報リスト上で、上記第1の接続要求信号に含まれる要求受諾機器の機器IDと一致した機器IDを含む機器情報の組に係る機器を上記要求受諾機器として識別し、上記機器情報リスト上で、上記識別された要求受諾機器に係る機器情報の組に含まれるIPアドレス及びポート番号を上記要求受諾機器に関連付けられたIPアドレス及びポート番号として識別するステップと、

上記識別された要求受諾機器に対して、上記識別されたIPアドレス及びポート番号を宛先として、上記受信された第1の接続要求信号に含まれる上記要求発行機器に関連付けられたIPアドレス及びポート番号を含む第2の接続要求信号を、上記機器登録信号に対する応答信号として送信するステップとを含むことを特徴とする。

【0045】

また、上記通信方法は、

上記識別するステップの後であって上記第2の接続要求信号を送信するステップの前に、上記要求受諾機器に第3の接続要求信号を送信し、上記第3の接続要求信号に対する応答信号として第2のTCP接続開始信号を上記要求受諾機器から受信することにより上記要求受諾機器との間において第2のTCP接続を確立するステップをさらに含み、

上記第2の接続要求信号を送信するステップは、上記確立された第2のTCP接続を用いて上記要求受諾機器に上記第2の接続要求信号を送信することを特徴とする。

【0046】

さらに、上記通信方法は、

上記第1の接続要求信号は、上記要求受諾機器のパスワード情報をさらに含み、

上記通信方法は、上記第1の接続要求信号に含まれた上記パスワード情報を上記第2の接続要求信号に付加して送信するステップをさらに含むことを特徴とする。

【0047】

またさらに、上記通信方法は、

上記第1の接続要求信号を受信するステップの前に、上記サーバ装置の正当性を証明するためのサーバ証明書情報を上記要求発行機器に送信するステップと、

上記要求発行機器から、上記サーバ証明書情報に応答して生成された第1の共通鍵作成情報を上記第1のTCP接続を用いて受信し、上記第1の共通鍵作成情報に応答して第2の共通鍵作成情報を生成し、上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて第1の通信用共通鍵を生成する一方、上記第2の共通鍵作成情報を上記要求発行機器に上記第1のTCP接続を用いて送信し、上記第1の通信用共通鍵と同一の通信用共通鍵を上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記要求発行機器に生成させることにより上記第1の通信用共通鍵を上記要求発行機器との間で共有するステップと、

上記要求発行機器から、上記第1の通信用共通鍵を用いて暗号化された上記第1の接続要求信号を、上記第1のTCP接続を用いて受信し、上記受信された第1の接続要求信号を、上記第1の通信用共通鍵を用いて復号化するステップと、

上記第2の接続要求信号を送信するステップの前に、上記要求受諾機器に上記サーバ証明書情報を送信するステップと、

上記要求受諾機器から、上記サーバ証明書情報に応答して生成された第3の共通鍵作成情報を上記第2のTCP接続を用いて受信し、上記第3の共通鍵作成情報に応答して第4の共通鍵作成情報を生成し、上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて第2の通信用共通鍵を生成する一方、上記第4の共通鍵作成情報を上記要求受諾機器に上記第2のTCP接続を用いて送信し、上記第2の通信用共通鍵と同一の通信用共

通鍵を上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記要求受諾機器に生成させることにより上記第2の通信用共通鍵を上記要求受諾機器との間で共有するステップと、

上記第1の接続要求信号を受信するステップの後であってかつ上記第2の接続要求信号を送信するステップの前に、上記第2の通信用共通鍵を用いて上記第2の接続要求信号を暗号化するステップとをさらに含むことを特徴とする。

【0048】

本発明の第6の態様に係る通信方法は、ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムに設けられ、上記サーバ装置及び上記要求受諾機器と通信する要求発行機器を用いた通信方法であって、

上記通信方法は、

上記サーバ装置に第1のTCP接続開始信号を送信することによって上記サーバ装置との間の第1のTCP接続を確立するステップと、

上記要求受諾機器の機器IDと上記要求発行機器に関連付けられたIPアドレス及びポート番号とを含む上記要求受諾機器への第1の接続要求信号を上記サーバ装置に上記第1のTCP接続を用いて送信するステップと、

上記要求発行機器と上記要求受諾機器との間の通信を要求する通信要求信号を上記要求受諾機器から受信した後に、上記通信要求信号に応答して上記要求発行機器と上記要求受諾機器との間の通信を受諾し、上記要求受諾機器との通信を開始するステップとを含むことを特徴とする。

【0049】

また、上記通信方法は、上記第1の接続要求信号は、上記要求受諾機器のパスワード情報をさらに含むことを特徴とする。

【0050】

さらに、上記通信方法は、

上記第1の接続要求信号を送信するステップの前に、上記サーバ装置から上記サーバ証明書情報を受信するステップと、

上記受信されたサーバ証明書情報を認証し、上記受信されたサーバ証明書情報が正規であるか否かを確認するステップと、

上記受信されたサーバ証明書情報を正規であると確認したとき、第1の共通鍵作成情報を生成し、上記生成された第1の共通鍵作成情報を上記第1のTCP接続を用いて上記サーバ装置に送信し、上記サーバ装置から、上記第1の共通鍵作成情報に応答して生成された第2の共通鍵作成情報を上記第1のTCP接続を用いて受信し、上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて第1の通信用共通鍵を生成する一方、上記第1の通信用共通鍵と同一の通信用共通鍵を上記第1の共通鍵作成情報及び上記第2の共通鍵作成情報に基づいて上記サーバ装置に生成させることにより上記第1の通信用共通鍵を上記サーバ装置との間で共有するステップと、

上記第1の接続要求信号を送信するステップの前に、上記第1の通信用共通鍵を用いて上記第1の接続要求信号を暗号化するステップとをさらに含むことを特徴とする。

【0051】

本発明の第7の態様に係る通信方法は、ネットワークにそれぞれ接続された要求発行機器と要求受諾機器とを含む複数の機器と、上記ネットワークに接続されたサーバ装置とを備えた通信システムに設けられ、上記サーバ装置及び上記要求発行機器と通信する要求受諾機器を用いた通信方法であって、

上記通信方法は、

上記要求受諾機器の機器IDを含む機器登録信号を上記サーバ装置に定期的に送信するステップと、

上記要求発行機器に関連付けられたIPアドレス及びポート番号を含む第2の接続要求信号を、上記機器登録信号に対する応答信号として上記サーバ装置から受信するステップ

と、

上記受信された第2の接続要求信号に含まれたIPアドレス及びポート番号が表す上記要求発行機器に、上記要求受諾機器と上記要求発行機器との間の通信を要求する通信要求信号を送信するステップと、

上記要求発行機器が上記通信要求信号に応答して上記要求受諾機器と上記要求発行機器との間の通信を受諾した後に、上記要求発行機器との通信を開始するステップとを含むことを特徴とする。

【0052】

また、上記通信方法は、

上記機器登録信号を上記サーバ装置に送信するステップの後であって上記第2の接続要求信号を受信するステップの前に、上記機器登録信号に対する応答信号として上記サーバ装置から第3の接続要求信号を受信し、上記第3の接続要求信号に対する応答信号として第2のTCP接続開始信号を上記サーバ装置に送信することにより上記サーバ装置との間において第2のTCP接続を確立するステップと、

上記確立された第2のTCP接続を用いて上記サーバ装置から上記第2の接続要求信号を受信するステップとをさらに含むことを特徴とする。

【0053】

さらに、上記通信方法において、

上記要求受諾機器は、上記要求受諾機器のパスワード情報を格納したパスワード情報格納手段を備え、

上記第2の接続要求信号はパスワード情報をさらに含み、

上記通信要求信号を送信するステップは、上記第2の接続要求信号に含まれたパスワード情報が、上記パスワード情報格納手段に格納された上記要求受諾機器のパスワード情報と一致している場合にのみ、上記要求発行機器に上記通信要求信号を送信することを特徴とする。

【0054】

またさらに、上記通信方法は、

上記第2の接続要求信号を受信するステップの前に、上記サーバ装置から上記サーバ証明書情報を受信するステップと、

上記受信されたサーバ証明書情報を認証し、上記受信されたサーバ証明書情報が正規であるか否かを確認するステップと、

上記受信されたサーバ証明書情報を正規であると確認したとき、第3の共通鍵作成情報を生成し、上記生成された第3の共通鍵作成情報を上記第2のTCP接続を用いて上記サーバ装置に送信し、上記サーバ装置から、上記第3の共通鍵作成情報に応答して生成された第4の共通鍵作成情報を上記第2のTCP接続を用いて受信し、上記第2の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて第2の通信用共通鍵を生成する一方、上記第2の通信用共通鍵と同一の通信用共通鍵を上記第3の共通鍵作成情報及び上記第4の共通鍵作成情報に基づいて上記サーバ装置に生成させることにより上記第2の通信用共通鍵を上記サーバ装置との間で共有するステップとをさらに含み、

上記第2の接続要求信号を受信するステップは、上記サーバ装置から、上記第2の通信用共通鍵を用いて暗号化された上記第2の接続要求信号を、上記第2のTCP接続を用いて受信し、上記受信された第2の接続要求信号を、上記第2の通信用共通鍵を用いて復号化するステップとをさらに含むことを特徴とする。

【0055】

本発明の第8の態様に係る通信方法は、上記サーバ装置と、上記要求発行機器及び上記要求受諾機器を含む複数の機器とを備えた通信システムを用いた通信方法であって、

上記複数の機器と上記サーバ装置とはそれぞれネットワークに接続され、

上記サーバ装置を用いた通信方法に係る各ステップと、上記要求発行機器を用いた通信方法に係る各ステップと、上記要求受諾機器を用いた通信方法に係る各ステップとを含むことを特徴とする。

【0056】

また、本発明の第9の態様に係るプログラムは、上記通信方法のうちの1つに係る各ステップを含むことを特徴とする。

【発明の効果】

【0057】

従って、本発明によれば、サーバ装置を利用することにより、プライベートIPアドレスをそれぞれ持つ異なったLAN上の機器である要求発行機器と要求受諾機器との間において、ピアツーピア通信を実現でき、かつ不正アクセスを許さないサーバ装置、要求発行機器、要求受諾機器、通信システム及び通信方法を容易に提供することができる。本発明はさらに、インターネットに接続されたコンピュータ又は機器に読み込まれたときに上記通信方法に係る各ステップを当該コンピュータ又は機器に実行させる、上記通信方法に係る各ステップを含むプログラムとして提供することもできる。

【発明を実施するための最良の形態】

【0058】

以下、本発明の実施形態について図1乃至図9を参照して説明する。

【0059】

図1は、本発明の実施形態に係る通信システムのネットワーク構成の一例を示すブロック図である。要求発行機器102とNAPT機能を有するルータ装置104aとは要求発行側LAN106aを構成し、要求発行側LAN106aは、ルータ装置104aのWAN側のポートにおいてインターネット(WAN)105に接続されている。同様に、要求受諾機器103とNAPT機能を有するルータ装置104bとは要求受諾側LAN106bを構成し、要求受諾側LAN106bは、ルータ装置104bのWAN側のポートにおいてインターネット(WAN)105に接続されている。サーバ装置101もまたインターネット(WAN)105に接続されている。

【0060】

本実施形態の通信システムによれば、要求発行機器102及び要求受諾機器103を含む、インターネット(WAN)105にそれぞれ接続された複数の機器と、インターネット105に接続されたサーバ装置101とを備え、要求発行側LAN106a内の要求発行機器102から、要求受諾側LAN106b内の要求受諾機器103への接続要求信号をサーバ装置101を介して転送し、かつ要求発行機器102と要求受諾機器103との間において通信を行う通信システムが提供される。この通信システムにおいて、サーバ装置101は、上記複数の機器にそれぞれ関連付けられたIPアドレス及びポート番号、並びに上記各機器の機器IDからなる上記各機器に係る機器情報の組を含む図9の機器情報リストを格納するための機器情報格納手段又はテーブルメモリ(図示せず。)を備え、要求受諾機器103は、要求受諾機器103に係る機器情報の組を含む機器登録パケット201をサーバ装置101に定期的に送信し、サーバ装置101は、機器登録パケット201を受信し、図2のステップS202及びS202Aにおいて、この受信された機器登録パケット201に含まれる要求受諾機器103に係る機器情報の組を上記機器情報格納手段に格納する。要求発行機器102は、要求受諾機器103との通信を行う際に、まず、第1の接続要求シーケンスのステップS203を実行し、ステップS203では、サーバ装置101にTCP接続開始パケット211を送信することによってサーバ装置101との間の第1のTCP接続を確立し、要求受諾機器103の機器IDと要求発行機器102に関連付けられたIPアドレス及びポート番号とを含む要求受諾機器103への接続要求パケット217を上記第1のTCP接続を用いてサーバ装置101に送信する。サーバ装置101は、接続要求パケット217を受信し、ステップS204において、受信された接続要求パケット217に含まれる要求受諾機器103の機器IDを上記機器情報リストから検索し、上記機器情報リスト上で、接続要求パケット217に含まれる要求受諾機器103の機器IDと一致した機器IDを含む機器情報の組に係る機器を要求受諾機器103として識別し、上記機器情報リスト上で、上記識別された要求受諾機器103に係る機器情報の組に含まれるIPアドレス及びポート番号を要求受諾機器103に関連付けられ

たIPアドレス及びポート番号として識別する。サーバ装置101は、ステップS205において、上記識別された要求受諾機器103に対して、上記識別されたIPアドレス及びポート番号を宛先として、受信された接続要求パケット217に含まれる要求発行機器102に関連付けられたIPアドレス及びポート番号を含む接続要求パケット226を、機器登録パケット201に対する応答信号として送信する。要求受諾機器103は、接続要求パケット226を受信し、受信された接続要求パケット226内のIPアドレス及びポート番号が表す要求発行機器102に対して、要求発行機器102と要求受諾機器103との間の通信を要求する通信要求信号としてTCP接続要求パケット208を送信し、要求発行機器102がTCP接続要求パケット208に回答して要求発行機器102と要求受諾機器103との間の通信を受諾すると、要求発行機器102と要求受諾機器103との間のデータ通信シーケンスのステップS209を開始する。

【0061】

本実施形態において、サーバ装置101、要求発行機器102及び要求受諾機器103は、専用の通信機器として構成されてもよく、又は、以下に説明される複数のステップを実行するためのプログラムによって動作される汎用のコンピュータとして構成されてもよい。

【0062】

本実施形態においては、図1に示すように、サーバ装置101にはグローバルIPアドレスとして“130.74.23.6”が割り当てられ、サーバ装置101は、それ自体のグローバルIPアドレスを格納したメモリ（図示せず。）と、機器情報リストを格納したテーブルメモリとを備えているものとする。要求発行機器102にはプライベートIPアドレスとして“192.168.1.11”が割り当てられ、要求受諾機器103にはプライベートIPアドレスとして“192.168.1.3”が割り当てられ、要求発行機器102は、それ自体のプライベートIPアドレス及びポート番号を格納したメモリ（図示せず。）を備え、要求受諾機器103は、それ自体のプライベートIPアドレス及びポート番号を格納したメモリ（図示せず。）を備えているものとする。ルータ装置104aにはグローバルIPアドレスとして“4.17.168.2”が割り当てられ、ルータ装置104bにはグローバルIPアドレスとして“202.204.16.13”が割り当てられているものとする。ルータ装置104aは、そのWAN側のポート番号及びそのグローバルIPアドレスと、要求発行機器102のプライベートIPアドレス及びポート番号とを含む、図12と同様のNAPTテーブル（図6を参照）の内容をその内部のテーブルメモリ（図示せず。）に格納している。ルータ装置104bもまた、そのWAN側のポート番号及びそのグローバルIPアドレスと、要求受諾機器103のプライベートIPアドレス及びポート番号とを含むNAPTテーブルの内容をその内部のテーブルメモリ（図示せず。）に格納している。

【0063】

また、要求発行機器102は、一意に割り当てられた機器ID“1051”をその内部のメモリに格納し、要求受諾機器103は、一意に割り当てられた機器ID“2133”をその内部のメモリに格納しているものとする。この機器IDは、ピアツーピア通信を行う本実施形態の各機器に対して一意に定められた識別情報であって、例えば、当該機器の製造業者によって割り当てられた識別番号、又はMACアドレスを用いることが可能であるが、それらに限定されない。

【0064】

さらに要求受諾機器103は、秘密情報であるパスワードをその内部のメモリに格納しているものとする。後述するように要求受諾機器103とのピアツーピア通信を行うことを希望する要求発行機器102は、要求受諾機器102のパスワード及び機器IDと、ルータ装置104aのグローバルIPアドレス及びWAN側ポート番号とを予め取得して内部のメモリに格納しておく必要がある。

【0065】

図2乃至図4は、図1の通信システムにおいて実行される通信シーケンスの一例を示す

シーケンス図である。また、図7及び図8に、図2乃至図4の通信シーケンスにおいて用いるいくつかのパケットの一例が示されている。

【0066】

要求受諾機器103は、定期的に、又は所定の周期を有して周期的に、機器IDをペイロードに持つ機器登録パケット201を、UDPを用いてサーバ装置101に送信する。図7(a)に示すように、要求受諾側LAN106b内において、機器登録パケット201のSAには“192.168.1.3”が書き込まれ、SPには“2000”が書き込まれている。機器登録パケット201はルータ装置104bを介してサーバ装置101に送信され、機器登録パケット201がルータ装置104bを通るときに、ルータ装置104bは、そのNAPT機能により、機器登録パケット201上のSAを“202.204.16.13”に変換し、機器登録パケット201上のSPを“3400”に変換する。図7(b)に示された、NAPT機能によって変換された後の機器登録パケット201は、インターネット(WAN)105経由によりサーバ装置101に送信される。

【0067】

サーバ装置101は、インターネット(WAN)105に接続された複数の機器にそれぞれ関連付けられたIPアドレス及びポート番号、並びに上記各機器の機器IDからなる上記各機器に係る機器情報の組を含む機器情報リストを格納するためのテーブルメモリ(図示せず。)を備えている。サーバ装置101は、受信した機器登録パケット201のSA、SP及びペイロードを参照し、ステップS202において、要求受諾機器103の機器IDと、ルータ装置104bのグローバルIPアドレスと、ルータ装置104bのWAN側のポート番号との組を、要求受諾機器103に対応する機器情報の組(すなわち機器情報リストの項目)として、サーバ装置101内のテーブルメモリに格納して保存する。本実施形態では、ルータ装置104bのグローバルIPアドレスとWAN側のポート番号とを、要求受諾機器103に関連付けられたIPアドレス及びポート番号として参照する。すなわち、サーバ装置101が要求受諾機器103に対してパケットを送信するとき、要求受諾機器103を含む要求受諾側LAN106bのグローバルIPアドレス及びWAN側ポート番号(従って、ルータ装置104bのグローバルIPアドレスとWAN側のポート番号)を宛先として参照する。図9に、サーバ装置101内のテーブルメモリに格納した機器情報リストの一例を示す。

【0068】

要求受諾機器103は、定期的に機器登録パケット201をサーバ装置101に送信するため、ルータ装置104bのグローバルIPアドレスもしくはWAN側ポート番号が変更になった場合でも、ステップS202や、同様のステップS202Aが実行されることにより、サーバ装置101上の機器情報リストは自動的に更新される。

【0069】

一方、要求発行機器102が要求受諾機器103とのデータ通信を所望する場合には、このことを伝達する接続要求メッセージを要求発行機器102から要求受諾機器103に伝送するために、要求発行機器102とサーバ装置101との間における第1の接続要求シーケンスのステップS203と、サーバ装置101におけるステップS204の実行及びパケット205の送信と、サーバ装置101と要求受諾機器103との間における第2の接続要求シーケンスのステップS206とを一連の処理として実行する。それによって、要求発行機器102による接続要求メッセージは、サーバ装置101が中継することにより、要求発行機器102から要求受諾機器103に転送される。要求発行機器102は、要求受諾機器103に対して接続要求メッセージを伝送するために、最初に、要求発行機器102とサーバ装置101との間において第1の接続要求シーケンスのステップS203を実行する。

【0070】

第1の接続要求シーケンスのステップS203は、要求受諾機器103のパスワード、要求受諾機器103の機器ID、要求発行機器102に関連付けられたIPアドレス及びポート番号のような秘密情報を伝送する必要があるため、本実施形態ではSSLを用いて

暗号化される。まず、後述の接続要求パケット 217 の送信などを暗号化するために用いられる SSL 通信について図 3 及び図 5 を用いて説明する。

【0071】

図 5 は、要求発行機器 102 及び要求受諾機器 103 に対してサーバ装置 101 の正当性を認証するための認証局装置 51 を示すブロック図であって、特に、サーバ装置 101 の正当性を証明するためのサーバ証明書データ 65 の配付及び認証方法を示す図である。図 5 において、ルータ装置 104a 及び 104b などは認証に関する説明では本質的ではないので省略した。図 5 において、認証局装置 (CA) 51 は、固有の CA 公開鍵 52 及び CA 秘密鍵 53 のペアを認証局装置 51 のメモリ (図示せず。) に格納し、また、サーバ装置 101 は、固有のサーバ秘密鍵 61 及びサーバ公開鍵 62 のペアと、認証局装置 51 によって発行されたサーバ証明書データ 65 とを、サーバ装置 101 のメモリ (図示せず。) に格納している。サーバ証明書データ 65 は、サーバ公開鍵 62 と、認証局装置 51 によって生成された署名 64 とを備えて構成される。

【0072】

図 2 の第 1 の接続要求シーケンスのステップ S203 及び第 2 の接続要求シーケンスのステップ S206 の処理を実行するために、まず予め、サーバ装置 101 は、以下に説明する処理に従って、認証局装置 51 からサーバ証明書データ 65 を発行してもらう必要がある。

【0073】

認証局装置 51 は、予め CA 公開鍵 52 と CA 秘密鍵 53 のペアを格納したメモリ (図示せず。) を備えている。サーバ装置 101 は、まずサーバ公開鍵 62 とサーバ秘密鍵 61 のペアを生成する。サーバ装置 101 は、サーバ公開鍵 62 とサーバ装置 101 に関する情報とを、サーバ証明書データ要求パケット 63 として認証局装置 51 に送信し、サーバ証明書データ 65 の発行を依頼する。認証局装置 51 は、サーバ証明書データ要求パケット 63 を受信すると、CA 秘密鍵 53 を用いて、サーバ装置 101 から受信した情報やその他必要な情報から署名 64 を生成し、サーバ装置 101 から受信した情報やその他必要な情報及び署名 64 を組み合わせたデータをサーバ証明書データ 65 としてサーバ装置 101 に対して発行する。発行されたサーバ証明書データ 65 は、サーバ証明書データ発行パケット 54 として、認証局装置 51 からサーバ装置 101 に送信される。サーバ装置 101 は、受信したサーバ証明書データ 65 をサーバ装置 101 の内部のメモリに格納しておく。

【0074】

また、クライアント装置である要求発行機器 102 及び要求受諾機器 103 は、予め認証局装置 51 から CA 公開鍵 52 を取得し、内部のメモリに格納しておく。なお、一般に、CA 公開鍵 52 は、認証局装置 51 の情報などと合わせた CA 証明書データパケット 55 の形態でクライアント装置 (すなわちサーバ装置 101 と通信する他の機器) などに配布される。要求発行機器 102 及び要求受諾機器 103 は、後述のように、サーバ装置 101 からのサーバ証明書データパケット 214 を介してサーバ証明書データ 65 を受信すると、要求発行機器 102 及び要求受諾機器 103 のそれぞれの証明書情報認証処理部 (図示せず。) を用いて、内部のメモリに格納している CA 公開鍵 52 でサーバ証明書データ 65 内の署名 64 を認証することにより、サーバ証明書データ 65 内のサーバ公開鍵 62 の正当性を確認することができる。

【0075】

実際に、要求発行機器 102 とサーバ装置 101 の間における秘密通信である第 1 の接続要求シーケンスのステップ S203 は、以下説明するように実行される。

【0076】

図 3 は、第 1 の接続要求シーケンス S203 の詳細な処理を示すシーケンス図であり、SSL 通信を用いて接続要求パケット 217 を送信するためのフローを示す図である。図 3 において、参照番号 73 は秘密通信に用いる通信用共通鍵を示す。

【0077】

サーバ装置 101 は、送受信する信号を暗号化しかつ復号化するための通信用共通鍵 73 及び 83 を生成し、生成した通信用共通鍵 73 を用いて、要求発行機器 102 との間で送受信する信号の暗号化及び復号化を実行し、通信用共通鍵 83 を用いて、要求受諾機器 103 との間で送受信する信号の暗号化及び復号化を実行する暗号通信処理部をさらに備えるものとする（図示せず。）。要求発行機器 102 は、送受信する信号を暗号化しかつ復号化するための通信用共通鍵 73 を生成し、生成した通信用共通鍵 73 を用いて、サーバ装置 101 との間で送受信する信号の暗号化及び復号化を実行する暗号通信処理部と、サーバ証明書データ 65 を認証する証明書情報認証処理部とをさらに備えるものとする（いずれも図示せず。）。

【0078】

SSL 通信において、クライアント側である要求発行機器 102 は、まず、TCP 接続開始パケット 211 を、ルータ装置 104 a を介してサーバ装置 101 に送信することによって、TCP 接続によるサーバ装置 101 との通信開始を要求する。ここで、図 6 に、ルータ装置 104 a の内部のメモリに格納している NAT テーブルの一例を示す。TCP 接続開始パケット 211 がルータ装置 104 a を通るときに、ルータ装置 104 a は、その NAT 機能を用いて、上記 NAT テーブルに従って、TCP 接続開始パケット 211 上の SA を“192.168.1.11”から“4.17.168.2”に変換し、TCP 接続開始パケット 211 上の SP を“1500”から“7000”に変換する。また、ルータ装置 104 a が要求発行機器 102 宛のパケットを受信するとき、当該パケットの DA に対して上記の変換と逆の変換を実行し、当該パケットの DP に対しても別の変換を実行して要求発行機器 102 に送信する。以下、本願明細書では、説明の簡単化のためにルータ装置 104 a の NAT 処理動作について言及することを省略するが、実際に要求発行機器 102 がインターネット（WAN）105 上のサーバ装置 101 又は他の機器との間でパケットを送受信する際には、常にルータ装置 104 a を介して送受信し、常にルータ装置 104 a が当該パケットに対して NAT 処理を実行するものとする。

【0079】

次いで、要求発行機器 102 とサーバ装置 101 は、暗号化仕様交渉のステップを実行することにより、秘密通信で用いる暗号化方式の仕様を相互に確認する。要求発行機器 102 は、最初に、TCP 接続開始パケット 211 で確立された TCP 接続を用いて、暗号化通信開始要求パケット（client_hello パケットともいう。）212 をサーバ装置 101 に送信する。暗号化通信開始要求パケット 212 の中には、使用可能な SSL のバージョン、使用可能な暗号化方式のリスト、セッション ID などが書き込まれ、その中に、要求発行機器 102 が生成した乱数である ClientHello.random も含まれている。サーバ装置 101 は、暗号化通信開始要求パケット 212 を受信し、通信を開始することを了承すると、TCP 接続開始パケット 211 で確立された TCP 接続を用いて暗号化通信開始応答パケット（server_hello パケットともいう。）213 を要求発行機器 102 に送信する。この暗号化通信開始応答パケット 213 は、使用する SSL のバージョン（要求発行機器 102 とサーバ装置 101 との両方がサポートする中で最も高いバージョン）、セッション ID、使用する暗号化方式などを含み、さらに、サーバ装置 101 において ClientHello.random と同様に生成された乱数である ServerHello.random を含んでいる。以下この第 1 の接続要求シーケンスのステップ S203 では、暗号化通信開始応答パケット 213 において指定された SSL のバージョン及び暗号化方式が使用される。これらの乱数 ClientHello.random 及び ServerHello.random は、32 ビットのタイムスタンプと、28 バイトの乱数（もしくは十分安全な疑似乱数）として、要求発行機器 102 とサーバ装置 101 それぞれが独立に生成する。これらの乱数 ClientHello.random 及び ServerHello.random をそれぞれ含む暗号化通信開始要求パケット 212 及び暗号化通信開始応答パケット 213 は、暗号化されずに送信される。

【0080】

次にサーバ装置 101 は、要求発行機器 102 にサーバ証明書データパケット 214 を送信する。要求発行機器 102 へのサーバ証明書データパケット 214 の送信は、暗号化

通信開始応答パケット 213 送信の後に限らず、後述される要求発行機器側通信用共通鍵作成情報パケット 215 の受信の前であれば（例えば、第 1 の接続要求シーケンスのステップ S203 の前）、いつでもよい。要求発行機器 102 の証明書情報認証処理部は、上記説明したように、内部に格納している CA 公開鍵 52 を用いて、送信されたサーバ証明書データパケット 214 内のサーバ証明書データ 65 が正規のものであるか否かを確認する。

【0081】

要求発行機器 102 は、その証明書情報認証処理部を用いて、送信されたサーバ証明書データ 65 が正規のものであると確認すると、要求発行機器側通信用共通鍵作成情報 71 及びサーバ装置側通信用共通鍵作成情報 72 の送受信を含む、共通鍵作成情報交換のステップを開始する。

【0082】

共通鍵作成情報交換のステップにおいて、最初に、要求発行機器 102 は、要求発行機器 102 の暗号通信処理部により要求発行機器側通信用共通鍵作成情報 71 を生成し、この生成された共通鍵作成情報 71 を含む要求発行機器側通信用共通鍵作成情報パケット 215 を、TCP 接続開始パケット 211 で確立された TCP 接続を用いてサーバ装置 101 に送信する。サーバ装置 101 は、送信された要求発行機器側通信用共通鍵作成情報パケット 215 に応答して、サーバ装置 101 の暗号通信処理部により、サーバ装置側通信用共通鍵作成情報 72 を生成し、この生成された共通鍵作成情報 72 を含むサーバ装置側通信用共通鍵作成情報パケット 216 を、TCP 接続開始パケット 211 で確立された TCP 接続を用いて要求発行機器 102 に送信する。要求発行機器 102 及びサーバ装置 101 は、双方の共通鍵作成情報 71 及び 72 に基づいて、それぞれの暗号通信処理部により同一の通信用共通鍵 73 をそれぞれ生成する。これにより、要求発行機器 102 とサーバ装置 101 とで通信用共通鍵 73 を共有することができる。

【0083】

共通鍵作成情報交換の実施形態は、SSL の鍵交換において使用される暗号化方式によって変化する。RSA 暗号化方式を使用する場合において、要求発行機器 102 の暗号通信処理部は、要求発行機器側通信用共通鍵作成情報 71 として、プリマスタシークレット (Pre Master Secret: PMS) と呼ばれる 48 バイトの乱数を生成し、サーバ証明書データ 65 に含まれるサーバ公開鍵 62 を用いて上記生成された PMS を暗号化する。次いで、要求発行機器 102 は、TCP 接続開始パケット 211 により確立された TCP 接続を用いて、暗号化された PMS をサーバ装置 101 に送信する。サーバ装置 101 は暗号通信処理部を使用し、暗号化された状態で受信した PMS を、自分の持っているサーバ秘密鍵 61 を用いて復号化することによって、送信された PMS を取得する。一方、サーバ装置側通信用共通鍵作成情報 72 の生成及び送信は省略される。サーバ装置 101 及び要求発行機器 102 は、この PMS を使って通信用共通鍵 73 を作成する（詳細後述）ことにより鍵共有を行う。

【0084】

ディフィーヘルマン (Diffie-Hellman) 暗号化方式を使用する場合は、要求発行機器 102 及びサーバ装置 101 は、ディフィーヘルマン鍵共有に用いるための 2 つのパラメータ（すなわち素数 p とその素数の原始根 g ）について予め同意している。サーバ証明書パケット 214 を受信した後、要求発行機器 102 は乱数 a を生成し、 p を法とする g^a の最小の正の剰余を要求発行機器側通信用共通鍵作成情報 71 として計算し、この共通鍵作成情報 71 を含む要求発行機器側通信用共通鍵作成情報パケット 215 をサーバ装置 101 に送信する一方、サーバ装置 101 は乱数 b を生成し、 p を法とする g^b の最小の正の剰余をサーバ装置側通信用共通鍵作成情報 72 として計算し、この共通鍵作成情報 72 を含むサーバ装置側通信用共通鍵作成情報パケット 216 を要求発行機器 102 に送信する。従って、互いに送信されるこれらの共通鍵作成情報が、ディフィーヘルマン公開鍵として用いられる。さらに、これらの共通鍵作成情報 71 及び 72 を送信するときに、要求発行機器 102 及びサーバ装置 101 のそれぞれの署名を付加してもよい。

【0085】

また、同じディフィーヘルマン暗号化方式でも、固定ディフィーヘルマン暗号化方式の場合には、サーバ装置101からの情報はサーバ証明書データ65に含まれる値を使用するので、この場合はサーバ装置側通信用共通鍵作成情報72の生成及び送信は省略される。

【0086】

以上のように、要求発行機器102及びサーバ装置101の間において共通鍵作成情報71及び72が交換されると、これらの共通鍵作成情報71及び72を用いることによって、後の通信において秘密鍵として用いるための通信用共通鍵73が生成される。通信用共通鍵73を生成するためには、互いに交換された共通鍵作成情報71及び72から、最初にプリマスタシークレット(PMS)を生成する。RSA暗号化方式の場合には、PMSは、上述のように要求発行機器側通信用共通鍵作成情報71である。ディフィーヘルマン暗号化方式の場合には、両者のディフィーヘルマン公開鍵を用いてPMSを生成する。すなわち、サーバ装置101は、受信した p を法とする g^a の最小の正の剰余を b 乗した値の、 p を法とする最小の正の剰余を計算してPMSとし、要求発行機器102は、受信した p を法とする g^b の最小の正の剰余を a 乗した値の、 p を法とする最小の正の剰余を計算してPMSとする。ディフィーヘルマン暗号化方式を用いた場合において、要求発行機器102及びサーバ装置101のそれぞれにおいて計算されたPMSは、 p を法とする g^{ab} の最小の正の剰余に等しい。

【0087】

PMSから通信用共通鍵73を作成するためには、MD5(Message Digest 5)とSHA(Secure Hash Algorithm)との2つのハッシュアルゴリズムを使用し、以下のように計算する。

【0088】

[数1]

```
共通鍵master_secret
= MD5(PMS || SHA('A' || PMS || ClientHello.random || ServerHello.random)) ||
MD5(PMS || SHA('BB' || PMS || ClientHello.random || ServerHello.random)) ||
MD5(PMS || SHA('CCC' || PMS || ClientHello.random || ServerHello.random))
```

【0089】

ここで「||」はビット列の連結を表す。

【0090】

以降、要求発行機器102及びサーバ装置101は、数1を用いて計算された共通鍵master_secretを通信用共通鍵73として用いて、接続要求パケット217の暗号化及び復号化を行うことにより、秘密通信を行うことが可能となる。すなわち、要求発行機器102及びサーバ装置101の間での通信用共通鍵73の共有が完了すると、要求発行機器102は、第1の接続要求パケット217を送信する前に、接続相手である要求受諾機器103の機器IDと、要求受諾機器103のパスワードと、要求発行機器102に関連付けられかつ通信に用いるためのIPアドレス及びポート番号を含むデータを通信用共通鍵73を用いて要求発行機器102の暗号通信手段により暗号化する。ここで、要求発行機器102に関連付けられたIPアドレス及びポート番号は、要求発行機器102を含む要求発行側LAN106aのグローバルIPアドレス及びWAN側ポート番号、すなわちルータ装置104aのWAN側グローバルIPアドレス及びWAN側ポート番号である。要求発行機器102は、この暗号化されたデータをペイロードとする接続要求パケット217を生成し、生成された接続要求パケット217を、TCP接続開始パケット211により確立されたTCP接続を用いてサーバ装置101に送信する。詳しくは、要求発行機器102は、図7(c)に示された接続要求パケット217をルータ装置104aに送信し、ルータ装置104aは受信した接続要求パケット217に対してNAPT処理を実行し、図7(d)に示されたNAPT処理後の接続要求パケット217をサーバ装置101に送信する。一方、サーバ装置101は、要求発行機器102との間で確立されたTCP接

続を用いて、要求発行機器 102 から、秘密情報として暗号化されたデータを含む接続要求パケット 217 を受信すると、通信用共通鍵 73 を用いて、上記暗号化されたデータをサーバ装置 101 の暗号通信処理部により復号化する。

【0091】

接続要求パケット 217 に書き込まれたルータ装置 104 a の WAN 側グローバル IP アドレスと WAN 側ポート番号は、後の TCP 接続開始パケット 208 とデータ通信シーケンスのステップ S209 に係るパケットとを送受信する際に使用される。すなわち、要求発行機器 102 が要求受諾機器 103 からの TCP 接続開始パケット 208 を受信して両者間の TCP 接続を確立し、要求発行機器 102 が、確立された TCP 接続上においてデータ通信シーケンスのステップ S209 に係るパケットを送受信する際（後述）に、ルータ装置 104 a の WAN 側グローバル IP アドレスと WAN 側ポート番号は、この送受信されるパケットに書き込まれており、このパケットに書き込まれたルータ装置 104 a の WAN 側グローバル IP アドレスと WAN 側ポート番号は、ルータ装置 104 a の NAT 機能を用いて要求発行機器 102 のプライベート IP アドレスとポート番号と相互変換できるものとする。

【0092】

例えば、要求発行機器 102 が要求受諾機器 103 からの TCP 接続開始パケット 208 を受信するためのポート番号を“1600”とすると、このときのルータ装置 104 a の NAT テーブルは図 6 のようになる。

【0093】

図 6 の NAT テーブルの 2 行目が、要求発行機器 102 が要求受諾機器 103 からの TCP 接続開始パケット 208 とその後のデータ通信シーケンスのステップ S209 におけるパケットとを受信するための変換テーブルである。要求受諾機器 103 は、グローバル IP アドレス“4. 17. 168. 2”及びポート番号“5000”を有するルータ装置 104 a に対して TCP 接続を確立するために TCP 接続開始パケット 208 を送信すると、ルータ装置 104 a の NAT 機能により、TCP 接続開始パケット 208 上に書き込まれた IP アドレスとポート番号が要求発行機器 102 のプライベート IP アドレスとルータ装置 104 a のポート番号とに変換されて、最終的に、要求受諾機器 103 は、要求発行機器 102 に対して TCP 接続を確立することができる。

【0094】

サーバ装置 101 は、接続要求パケット 217 を受信すると、ステップ S204 において、内部のメモリに格納している図 9 の機器情報リスト内の複数の機器情報の組を参照し、受信された接続要求パケット 217 に含まれた要求受諾機器 103 の機器 ID “2133”を機器情報リストから検索する。機器情報リスト上で“2133”と一致した機器 ID が見つかり、サーバ装置 101 は、この機器 ID “2133”を含む機器情報の組に係る機器を接続相手の要求受諾機器 103 として識別し、また、機器情報リスト上で、識別された要求受諾機器 103 に係る機器情報の組に含まれる IP アドレス及びポート番号を要求受諾機器 103 に関連付けられた IP アドレス及びポート番号として識別する。サーバ装置 101 は、受信された接続要求パケット 217 に含まれた要求発行機器 102 に関連付けられた IP アドレス及びポート番号と要求受諾機器 103 のパスワードとを要求受諾機器 103 に対してすぐには送信せず、まず、要求受諾機器 103 に関連付けられている（すなわち、機器 ID “2133”と同じ機器情報の組に含まれた）IP アドレス“202. 204. 16. 13”及びポート番号“3400”を宛先として、接続要求通知パケット 205 を UDP を用いて送信する。接続要求通知パケット 205 は、機器登録パケット 201 に対する応答信号としてルータ装置 104 b に送信されるため、ルータ装置 104 b において IP アドレスとポート番号の変換が行われ、要求受諾機器 103 に到達できる。図 8（a）及び（b）に示すように、接続要求通知パケット 205 は、接続要求通知を示すパケットであることを示す接続要求通知フラグを含んでいる。

【0095】

要求受諾機器 103 は、接続要求通知パケット 205 を受信すると、サーバ装置 101

との間において第2の接続要求シーケンスS206を実行する。

【0096】

図4は、第2の接続要求シーケンスS206の詳細な処理を示すシーケンス図である。第2の接続要求シーケンスのステップS206もまた、第1の接続要求シーケンスのステップS203と同様に、要求受諾機器103のパスワード、要求発行機器102に関連付けられたIPアドレス及びポート番号のような秘密情報を伝送する必要があるので、本実施形態ではSSLを用いて暗号化される。ここで、要求受諾機器103は、送受信する信号を暗号化しかつ復号化するための通信用共通鍵83を生成し、生成した通信用共通鍵83を用いて、サーバ装置101との間で送受信する信号の暗号化及び復号化を実行する暗号通信処理部と、サーバ証明書データ65を認証する証明書情報認証処理部とをさらに備えるものとする（いずれも図示せず。）。サーバ装置101と要求受諾機器103との間での秘密通信である第2の接続要求シーケンスのステップS206は、以下説明するように実行される。

【0097】

SSL通信において、クライアント側である要求受諾機器103は、まず、TCP接続開始パケット221を、ルータ装置104bを介してサーバ装置101に送信することによって、TCP接続によるサーバ装置101との通信開始を要求する。TCP接続開始パケット221がルータ装置104bを通るときに、ルータ装置104bは、機器登録パケット201の送信時に用いたNAPT機能を使用し、TCP接続開始パケット221上のSA及びSPを変換する。また、ルータ装置104bが要求受諾機器103宛のパケットを受信するとき、当該パケットのDAに対して上記の変換と逆の変換を実行し、当該パケットのDPに対しても別の変換を実行して要求受諾機器103に送信する。以下、本願明細書では、説明の簡単化のためにルータ装置104bのNAPT処理動作について言及することを省略するが、実際に要求受諾機器103がパケットを送受信する際には、常にルータ装置104bを介して送受信し、常にルータ装置104bが当該パケットに対してNAPT処理を実行するものとする。

【0098】

次いで、要求受諾機器103とサーバ装置101は、暗号化仕様交渉のステップを実行することにより、秘密通信で用いる暗号化方式の仕様を相互に確認する。要求受諾機器103は、最初に、TCP接続開始パケット221で確立されたTCP接続を用いて、暗号化通信開始要求パケット（client_helloパケットともいう。）222をサーバ装置101に送信する。暗号化通信開始要求パケット222の中には、使用可能なSSLのバージョン、使用可能な暗号化方式のリスト、セッションIDなどが書き込まれ、その中に、要求受諾機器103が生成した乱数であるClientHello.randomも含まれている。サーバ装置101は、要求受諾機器103から暗号化通信開始要求パケット222を受信すると、TCP接続開始パケット221で確立されたTCP接続を用いて暗号化通信開始応答パケット（server_helloパケットともいう。）223を要求受諾機器103に送信する。この暗号化通信開始応答パケット223は、使用するSSLのバージョン（要求発行機器102とサーバ装置101との両方がサポートする中で最も高いバージョン）、セッションID、使用する暗号化方式などを含み、さらに、サーバ装置101において生成された乱数であるServerHello.randomを含んでいる。以下この第2の接続要求シーケンスのステップS206では、暗号化通信開始応答パケット223において指定されたSSLのバージョン及び暗号化方式が使用される。これらの乱数ClientHello.random及びServerHello.randomは、32ビットのタイムスタンプと、28バイトの乱数（もしくは十分安全な疑似乱数）として、要求受諾機器103とサーバ装置101それぞれが独立に生成する。これらの乱数ClientHello.random及びServerHello.randomをそれぞれ含む暗号化通信開始要求パケット222及び暗号化通信開始応答パケット223は、暗号化されずに送信される。

【0099】

次にサーバ装置101は、要求受諾機器103にサーバ証明書データパケット214を送信する。要求受諾機器103へのサーバ証明書データパケット214の送信は、暗号化

通信開始応答パケット 223 送信の後に限らず、後述される要求受諾機器側通信用共通鍵作成情報パケット 224 の受信の前であれば（例えば、第 2 の接続要求シーケンスのステップ S206 の前）、いつでもよい。要求受諾機器 103 の証明書情報認証処理部は、図 5 を参照して要求発行機器 102 の場合について説明したときと同様に、内部に格納している CA 公開鍵 52 を用いて、送信されたサーバ証明書データパケット 214 内のサーバ証明書データ 65 が正規のものであるか否かを確認する。

【0100】

要求受諾機器 103 は、その証明書情報認証処理部を用いて、送信されたサーバ証明書データ 65 が正規のものであると確認すると、以下、要求受諾機器側通信用共通鍵作成情報 81 及びサーバ装置側通信用共通鍵作成情報 82 の送受信を含む、共通鍵作成情報交換のステップを開始する。

【0101】

共通鍵作成情報交換のステップにおいて、最初に、要求受諾機器 103 は、要求受諾機器 103 の暗号通信処理部により要求受諾機器側通信用共通鍵作成情報 81 を生成し、この生成された共通鍵作成情報 81 を含む要求受諾機器側通信用共通鍵作成情報パケット 224 を、TCP 接続開始パケット 221 で確立された TCP 接続を用いてサーバ装置 101 に送信する。サーバ装置 101 は、送信された要求受諾機器側通信用共通鍵作成情報パケット 224 に応答して、サーバ装置 101 の暗号通信処理部により、サーバ装置側通信用共通鍵作成情報 82 を生成し、この生成された共通鍵作成情報 82 を含むサーバ装置側通信用共通鍵作成情報パケット 225 を、TCP 接続開始パケット 211 で確立された TCP 接続を用いて要求発行機器 102 に送信する。要求発行機器 102 及びサーバ装置 101 は、双方の共通鍵作成情報 81 及び 82 に基づいて、それぞれの暗号通信処理部により同一の通信用共通鍵 83 をそれぞれ生成する。通信用共通鍵 83 を生成するためには、第 1 の接続要求シーケンスのステップ S203 の場合について説明されたときと同様に RSA 暗号化方式又はディフィー・ヘルマン暗号化方式などを用いて、生成された共通鍵作成情報 81 及び 82 を互いに交換し、サーバ装置 101 及び要求受諾機器 103 の各暗号通信処理部は、これらの共通鍵作成情報 81 及び 82 を用いることによって、後の通信で秘密鍵として用いるための通信用共通鍵 83 をそれぞれ生成する。

【0102】

これにより、サーバ装置 101 及び要求受諾機器 103 の間において通信用共通鍵 83 を共有することができ、サーバ装置 101 及び要求受諾機器 103 は、通信用共通鍵 83 を用いて、接続要求パケット 226 の暗号化及び復号化を行うことで、秘密通信を行うことが可能となる。すなわち、第 1 の接続要求パケット 217 を受信した後であってかつ第 2 の接続要求パケット 226 を送信する前に、サーバ装置 101 及び要求受諾機器 103 の間での通信用共通鍵 83 の共有が完了すると、サーバ装置 101 は、接続要求パケット 217 に含まれている要求受諾機器 103 のパスワードと、通信に用いるルータ装置 104a のグローバル IP アドレス “4. 17. 168. 2” とポート番号 “5000” とを含むデータを通信用共通鍵 83 を用いてサーバ装置 101 の暗号通信処理部により暗号化する。サーバ装置 101 は、この暗号化されたデータをペイロードとして含む接続要求パケット 226 を生成し、生成された接続要求パケット 226 を、機器登録パケット 201 に対する応答信号として、TCP 接続開始パケット 221 により確立された TCP 接続を用いて要求受諾機器 103 に送信する。詳しくは、サーバ装置 101 は、図 2 のステップ S204 においてサーバ装置 101 の機器情報リスト内で要求受諾機器 103 のものとして識別された IP アドレス及びポート番号を宛先として、図 8 (d) に示された接続要求パケット 226 をルータ装置 104b に送信し、ルータ装置 104b は受信した接続要求パケット 226 に対して NAT 処理を実行し、図 8 (c) に示された NAT 処理後の接続要求パケット 226 を要求受諾機器 103 に送信する。一方、要求受諾機器 103 は、サーバ装置 101 との間において確立された TCP 接続を用いて、サーバ装置から、秘密情報として暗号化されたデータを含む接続要求パケット 226 を受信すると、通信用共通鍵 83 を用いて、上記暗号化されたデータを要求受諾機器 103 の暗号通信処理部によ

り復号化する。以上のようにして、要求発行機器 102 が要求受諾機器 103 とのデータ通信を所望することを伝達する接続要求メッセージが、最終的に、要求発行機器 102 から要求受諾機器 103 に伝送される。

【0103】

再び図 2 を参照すると、要求受諾機器 103 は、ステップ S207 において、接続要求パケット 226 に含まれているパスワードが、要求受諾機器 103 内のメモリに格納された要求受諾機器 103 のパスワードと一致した正しいものであるか否かを認証する。パスワードが正しい場合かつそのときに限って、要求受諾機器 103 は、接続要求パケット 226 に含まれている IP アドレス “4. 17. 168. 2” 及びポート番号 “5000” に関連付けられた要求発行機器 102 に対して、要求発行機器 102 と要求受諾機器 103 との間の TCP 接続による通信を要求するための通信要求信号として、TCP 接続開始パケット 208 をルータ装置 104a に送信する。TCP 接続開始パケット 208 は、前述のようにルータ装置 104a の NAT 機能により要求発行機器 102 に到達し、要求受諾機器 103 は、要求発行機器 102 との TCP 接続を確立することができる。

【0104】

要求発行機器 102 が TCP 接続開始パケット 208 に応答して要求発行機器 102 と要求受諾機器 103 との間の通信を受諾すると、以降、要求発行機器 102 と要求受諾機器 103 とは、TCP 接続開始パケット 208 により確立された TCP 接続を用いてデータ通信シーケンスのステップ S209 を行えるようになる。

【0105】

以上のようにして、サーバ装置 101 を利用することで、プライベート IP アドレスを持つ異なった LAN106a 及び 106b 上の機器である要求発行機器 102 と要求受諾機器 103 との間でデータ通信を行うことができるようになる。

【0106】

なお、要求発行機器 102 がグローバル IP アドレスを保有し、直接インターネット (WAN) 105 に接続されている場合でも、同様の動作で要求発行機器 102 と要求受諾機器 103 との間において通信を行うことができる。また、要求受諾機器 103 がグローバル IP アドレスを保有し、直接インターネット (WAN) 105 に接続されている場合でも、同様の動作で要求発行機器 102 と要求受諾機器 103 との間において通信を行うことができる。いずれの場合でも、ルータ装置によって IP アドレスやポート番号の変換が行われないだけで、それ以外の動作は上記説明と同様の動作となる。

【0107】

本実施形態では、サーバ装置 101、要求発行機器 102 及び要求受諾機器 103 はインターネット (WAN) 105 に接続されているが、本発明の実施形態はそれに限定されず、サーバ装置 101、要求発行機器 102 及び要求受諾機器 103 は、その他の公開されたネットワーク及び/又は専用のネットワークに接続されるように構成されてもよい。

【0108】

また、ルータ装置 104a やルータ装置 104b が、NAT 機能ではなく NAT 機能のみ有している場合でも同様の動作で要求発行機器 102 と要求受諾機器 103 との間における通信を行うことができる。この場合、ルータ装置においてポート番号の変換は行われない。

【0109】

また、要求発行機器 102 は、TCP 接続開始パケット 208 を受信するための IP アドレスとポート番号の組み合わせを常に図 6 のような NAT テーブルに設定したままでもよいし、又は、第 1 の接続要求シーケンス S203 において TCP 接続開始パケット 211 を送信する際にこの組み合わせを NAT テーブルに設定し、データ通信シーケンスのステップ S209 が終了するとこの組み合わせを NAT テーブルから削除するようにしてもよい。NAT テーブルの設定は、静的 NAT を用いてもよいし、ユニバーサル・プラグ・アンド・プレイ (Universal Plug and Play) などの機能を用いてもよい。

【0110】

また、第1の接続要求シーケンスのステップS203におけるTCP接続開始パケット211により開始されるTCP接続を介した通信と、第2の接続要求シーケンスのステップS206におけるTCP接続開始パケット221により開始されるTCP接続を介した通信とは、SSL (Secure Sockets Layer) とは異なる暗号化通信を用いてもよい。又は、これらステップS3及びS6におけるTCP通信の暗号化は省略されてもよい。この場合、ステップS3において、要求発行機器102は、TCP接続開始パケット211を送信してTCP接続を確立した後すぐに接続要求パケット217を送信し、ステップS6において、サーバ装置101は、TCP接続開始パケット221を受信した後すぐに接続要求パケット226を送信してもよい。

【0111】

また、データ通信シーケンスのステップS209の処理は、ステップS202及びS206と同様に、SSLなどの暗号化通信を用いて実行してもよい。また、ステップS209におけるデータの送受信は、UDPなど他の伝送プロトコルを用いて実行してもよい。

【0112】

また、図7及び図8に示す機器登録パケット201、接続要求パケット217、接続要求通知パケット205及び接続要求パケット226は一例であって、他のフィールドが含まれていてもよいし、各フィールドの順序が異なってもよい。

【0113】

また、図1から図9で用いているIPアドレス、ポート番号及び機器IDは一例であって、他の値であっても構わない。

【0114】

本発明はさらに別の実施形態として、図2乃至図4に示された処理に係る各ステップを含むプログラムとして提供してもよく、あるいは、上記プログラムを記録し、コンピュータが読み取り可能な記録媒体として提供してもよい。この場合、上記プログラムを、インターネットに接続されたコンピュータ又は機器に読み込ませて、上記プログラム中の各ステップを当該コンピュータ又は機器に実行させることにより、当該コンピュータ又は機器を、以上説明された実施形態におけるサーバ装置101、要求発行機器102、及び／又は要求受諾機器103として動作させることができる。上記プログラムを記録した記録媒体の例として、CD-ROM及びDVD-ROM等の光記録媒体、フレキシブルディスク及びハードディスク等の磁気記録媒体、又は半導体記憶装置などが可能であるが、それらに制限されない。また、上記プログラムは、インターネットなどのネットワークを介して分配されてもよい。

【産業上の利用可能性】

【0115】

以上説明したように、本発明によれば、インターネット (WAN) に接続された異なるLAN上の機器同士で、不正アクセスができないピアツーピア通信を容易に実現する通信システムを提供することができる。

【図面の簡単な説明】

【0116】

【図1】 本発明の実施形態に係る通信システムのネットワーク構成を示すブロック図である。

【図2】 図1の通信システムにおいて実行される通信シーケンスの一例を示すシーケンス図である。

【図3】 図2の第1の接続要求シーケンスS203の詳細な処理を示すシーケンス図である。

【図4】 図2の第2の接続要求シーケンスS206の詳細な処理を示すシーケンス図である。

【図5】 図1の要求発行機器102及び要求受諾機器103に対してサーバ装置101の正当性を認証するための認証局装置51を示すブロック図である。

【図6】 図1のルータ装置104aの内部のメモリに格納しているNAPTテーブル

の一例を示す表である。

【図 7】 (a) は図 2 の LAN 側での機器登録パケット 201 の構成を示す図であり、(b) は図 2 の WAN 側での機器登録パケット 201 の構成を示す図であり、(c) は図 3 の LAN 側での接続要求パケット 217 の構成を示す図であり、(d) は図 3 の WAN 側での接続要求パケット 217 の構成を示す図である。

【図 8】 (a) は図 2 の LAN 側での接続要求通知パケット 205 の構成を示す図であり、(b) は図 2 の WAN 側での接続要求通知パケット 205 の構成を示す図であり、(c) は図 4 の LAN 側での接続要求パケット 226 の構成を示す図であり、(d) は図 4 の WAN 側での接続要求パケット 226 の構成を示す図である。

【図 9】 図 1 のサーバ装置 101 で保存している機器情報リストの一例を示す表である。

【図 10】 従来技術の通信システムのネットワーク構成の一例を示すブロック図である。

【図 11】 ルータ装置 104 の NAT 機能を用いた通信の通信シーケンスの一例を示すシーケンス図である。

【図 12】 ルータ装置 104 の NAT テーブルの一例を示す表である。

【図 13】 図 10 の通信システムの通信シーケンスの一例を示すシーケンス図である。

【符号の説明】

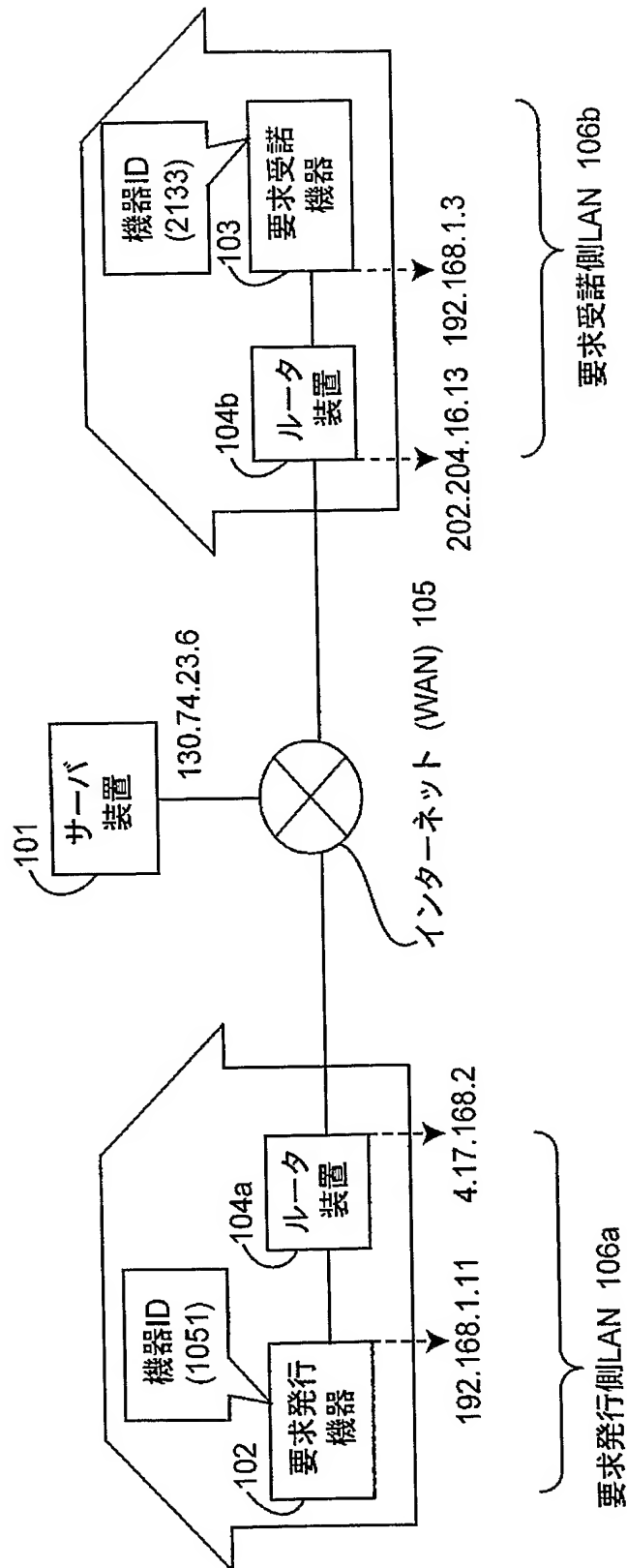
【0117】

- 51…認証局 (CA) 装置、
- 52…CA 公開鍵、
- 53…CA 秘密鍵、
- 54…サーバ証明書データ発行パケット、
- 55…CA 証明書データパケット、
- 61…サーバ秘密鍵、
- 62…サーバ公開鍵、
- 63…サーバ証明書データ要求パケット、
- 64…署名、
- 65…サーバ証明書データ、
- 71…要求発行機器側通信用共通鍵作成情報、
- 72…サーバ装置側通信用共通鍵作成情報、
- 81…要求受諾機器側通信用共通鍵作成情報、
- 82…サーバ装置側通信用共通鍵作成情報、
- 73, 83…通信用共通鍵、
- 101…サーバ装置、
- 102…要求発行機器、
- 103…要求受諾機器、
- 104a, 104b…ルータ装置、
- 105…インターネット (WAN)、
- 106a, 106b…LAN、
- 201…機器登録パケット、
- 205…接続要求通知パケット、
- 208, 211, 221…TCP 接続開始パケット、
- 212, 222…暗号化通信開始要求パケット、
- 213, 223…暗号化通信開始応答パケット、
- 214…サーバ証明書データパケット、
- 215…要求発行機器側通信用共通鍵作成情報パケット、
- 216, 225…サーバ装置側通信用共通鍵作成情報パケット、
- 217, 226…接続要求パケット、

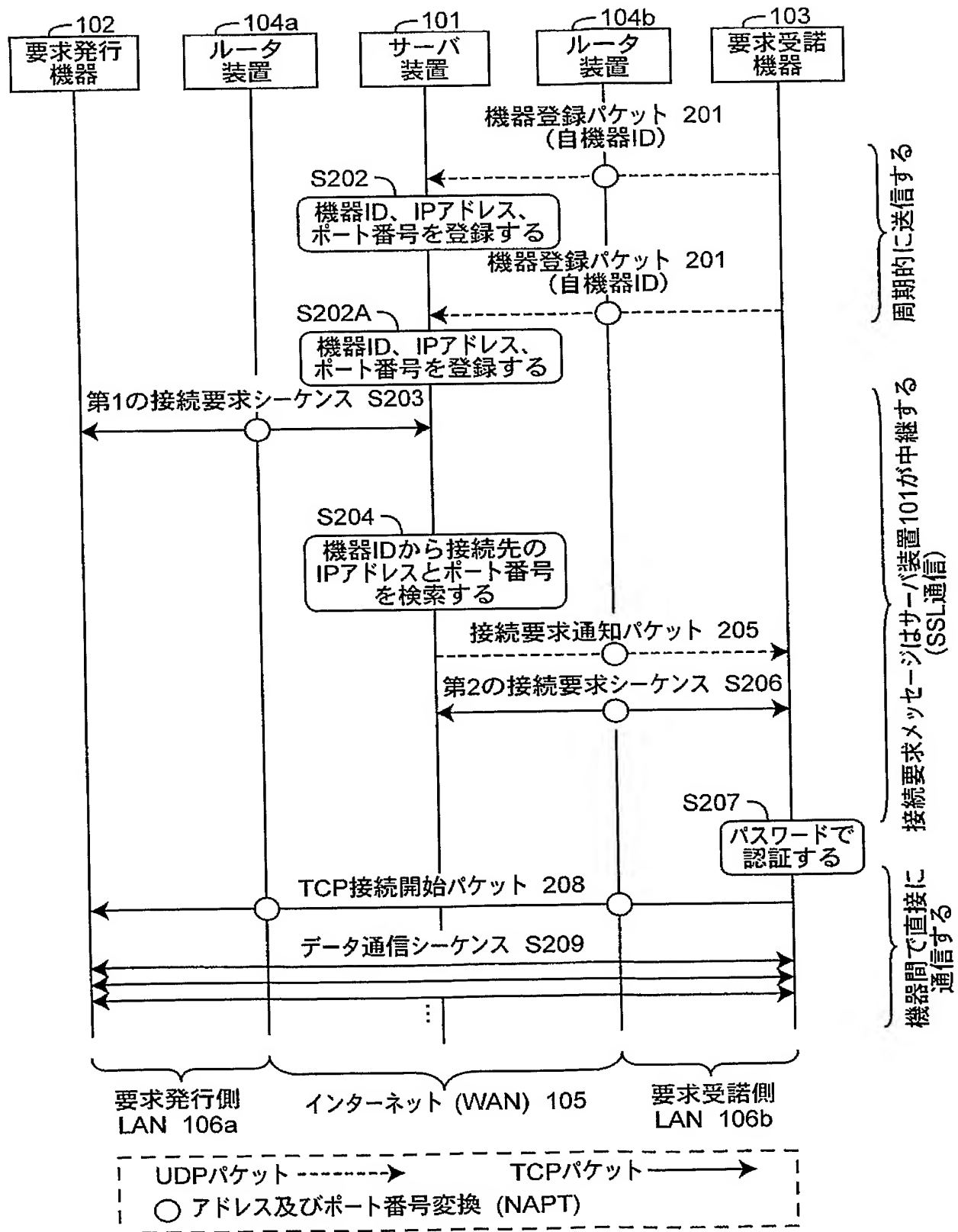
2 2 4 …要求受諾機器側通信用共通鍵作成情報パケット。

【書類名】 図面
【図 1】

実施形態

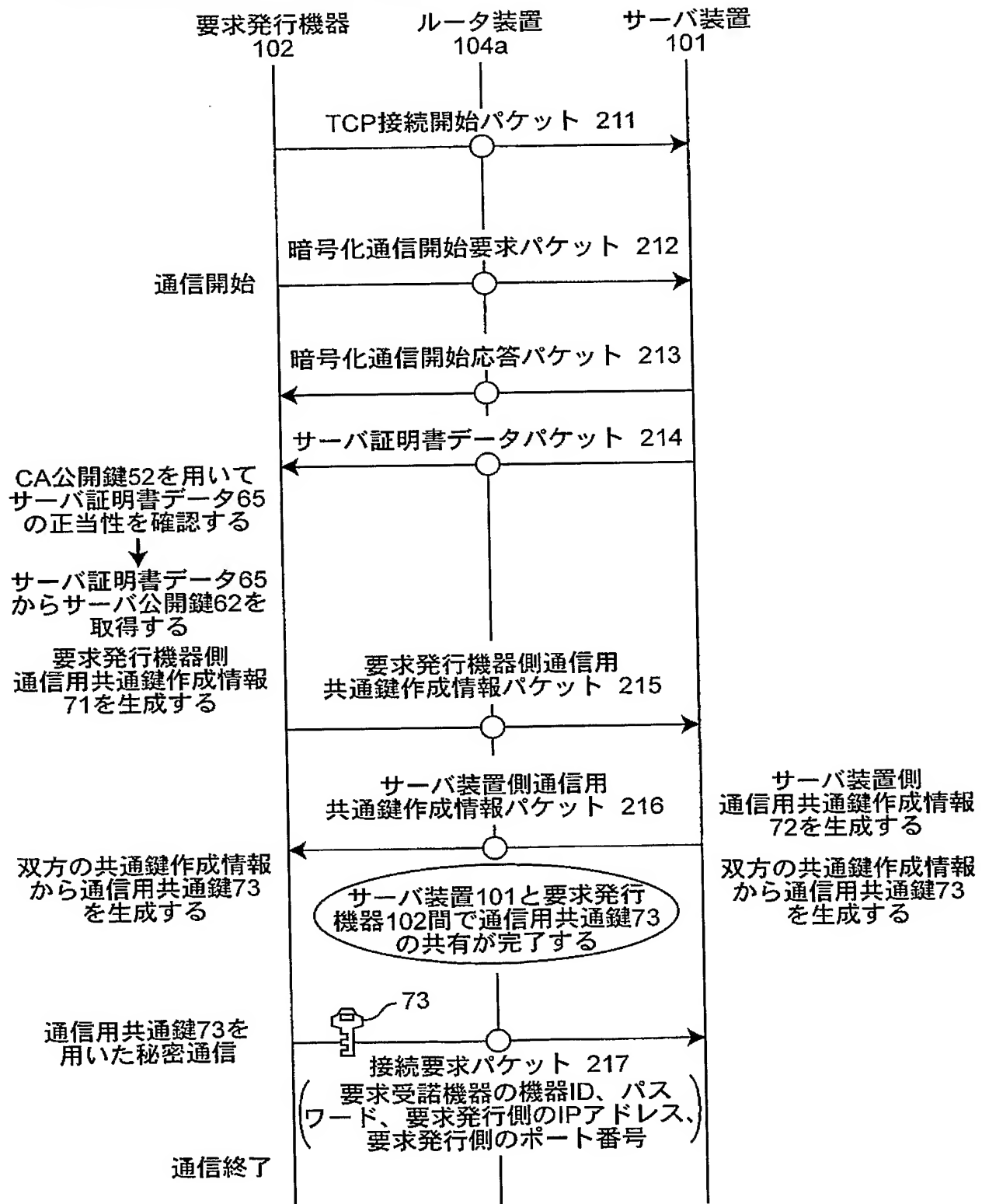


【図 2】



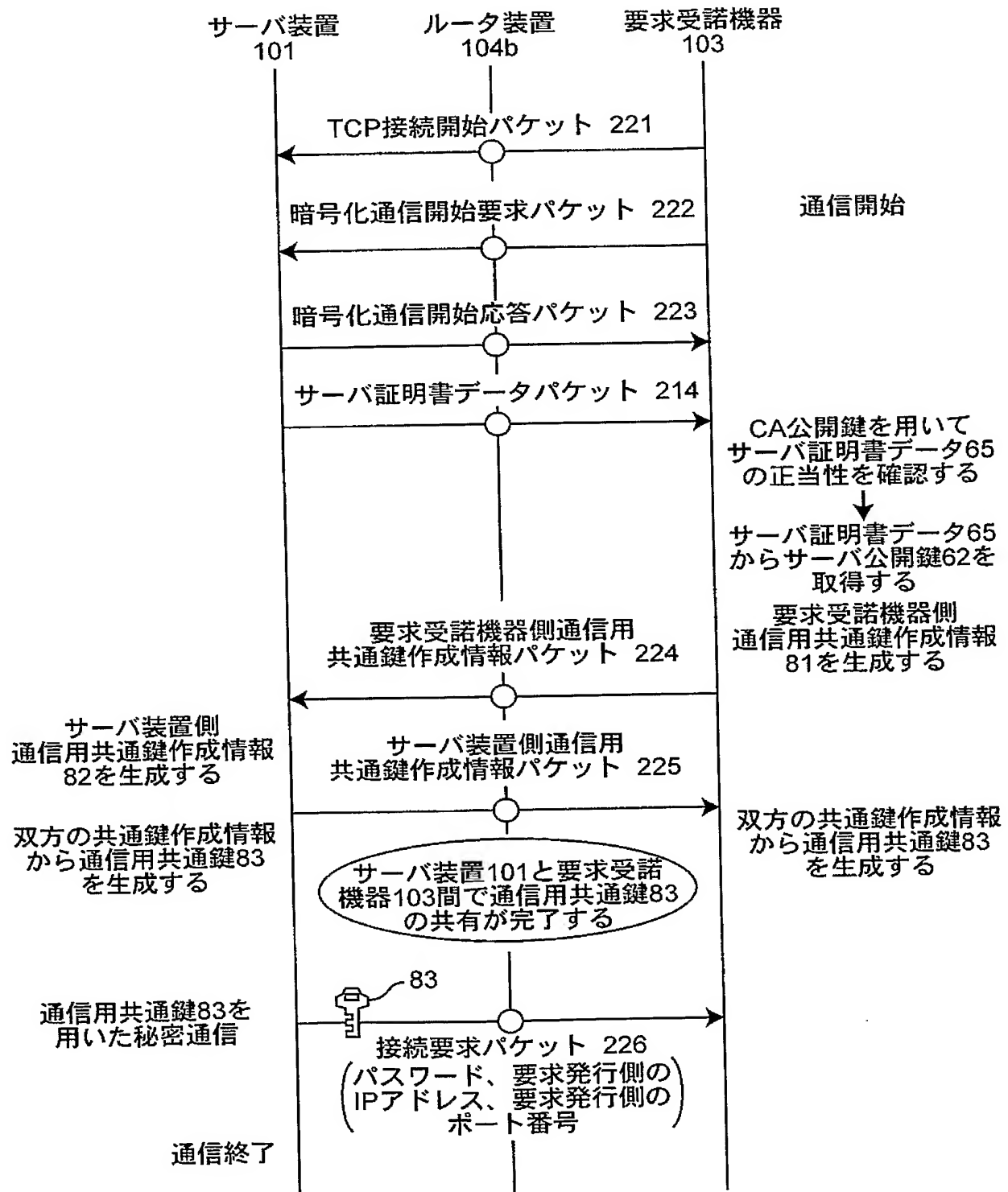
【図3】

第1の接続要求シーケンス S203

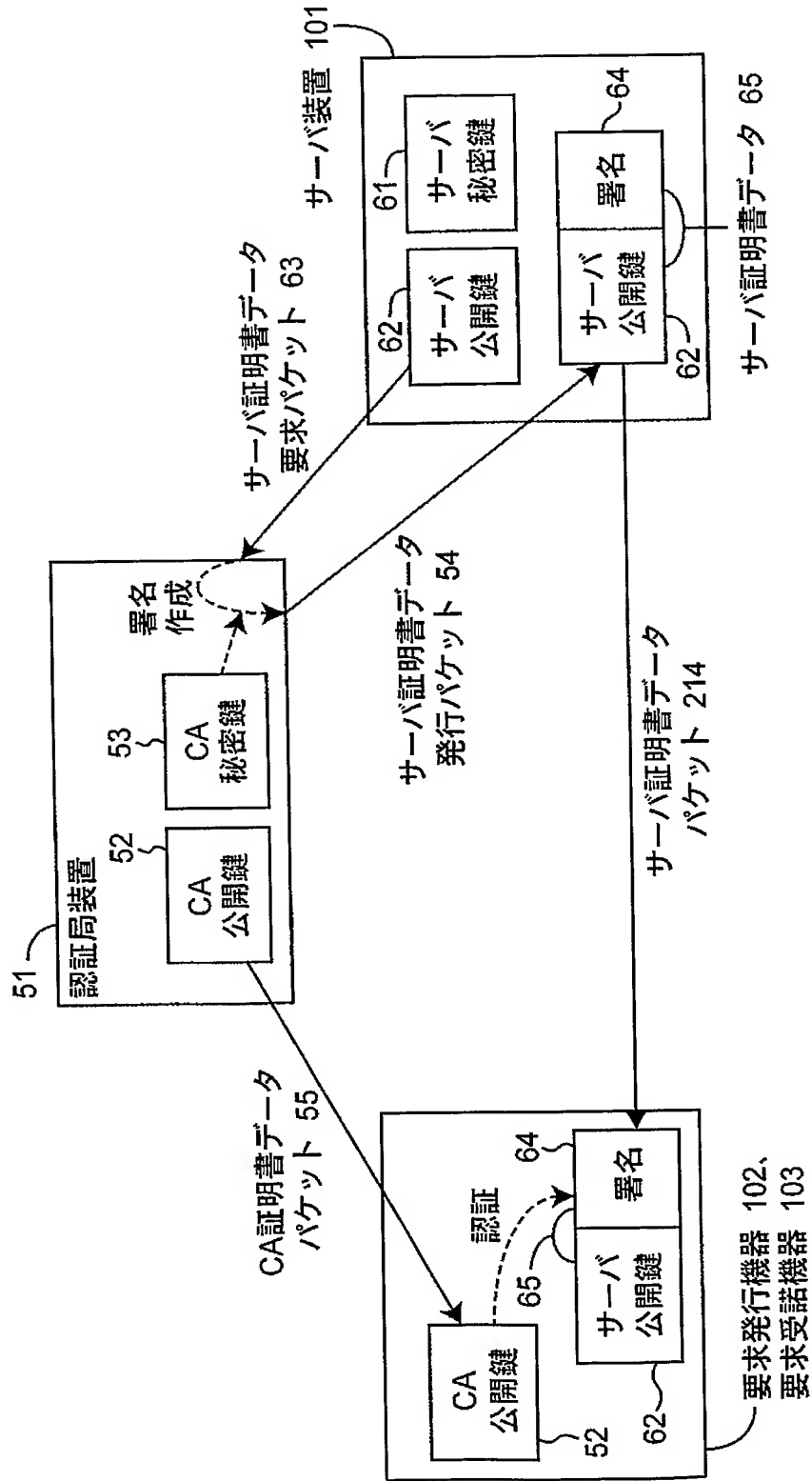


【図 4】

第2の接続要求シーケンス S206



【図 5】



【図 6】

LAN 機器アドレス	WAN ルータアドレス	LAN 機器ポート番号	WAN ルータポート番号
192.168.1.11	4.17.168.2	1500	7000
192.168.1.11	4.17.168.2	1600	5000
---	---	---	---

←サーバ装置101とのTCP通信用

←要求受諾機器103とのTCP通信用

【図 7】

(a) 機器登録パケット 201 (LAN側)

SA= 192.168.1.3
DA= 130.74.23.6
SP= 2000
DP= 1200
要求受諾機器103の機器ID (2133)

(b) 機器登録パケット 201 (WAN側)

SA= 202.204.16.13
DA= 130.74.23.6
SP= 3400
DP= 1200
要求受諾機器103の機器ID (2133)

(c) 接続要求パケット 217 (LAN側)

SA= 192.168.1.11
DA= 130.74.23.6
SP= 1500
DP= 1201
要求受諾機器103の機器ID (2133)
要求受諾機器103のパスワード
要求発行側LAN106aのIPアドレス (4.17.168.2)
要求発行側LAN106aのポート番号 (5000)

(d) 接続要求パケット 217 (WAN側)

SA= 4.17.168.2
DA= 130.74.23.6
SP= 7000
DP= 1201
要求受諾機器103の機器ID (2133)
要求受諾機器103のパスワード
要求発行側LAN106aのIPアドレス (4.17.168.2)
要求発行側LAN106aのポート番号 (5000)

SA: 発信元アドレスフィールド、DA:宛先アドレスフィールド
 SP:発信元ポート番号フィールド、DP:宛先ポート番号フィールド

【図 8】

(a) 接続要求通知パケット 205 (LAN側)

SA= 130.74.23.6
DA= 192.168.1.3
SP= 1200
DP= 2000
接続要求通知フラグ

(b) 接続要求通知パケット 205 (WAN側)

SA= 130.74.23.6
DA= 202.204.16.13
SP= 1200
DP= 2400
接続要求通知フラグ

(c) 接続要求パケット 226 (LAN側)

SA= 130.74.23.6
DA= 192.168.1.3
SP= 1300
DP= 2600
要求受諾機器103のパスワード
要求発行側LAN106aのIPアドレス (4.17.168.2)
要求発行側LAN106aのポート番号 (5000)

(d) 接続要求パケット 226 (WAN側)

SA= 130.74.23.6
DA= 202.204.16.13
SP= 1300
DP= 2401
要求受諾機器103のパスワード
要求発行側LAN106aのIPアドレス (4.17.168.2)
要求発行側LAN106aのポート番号 (5000)

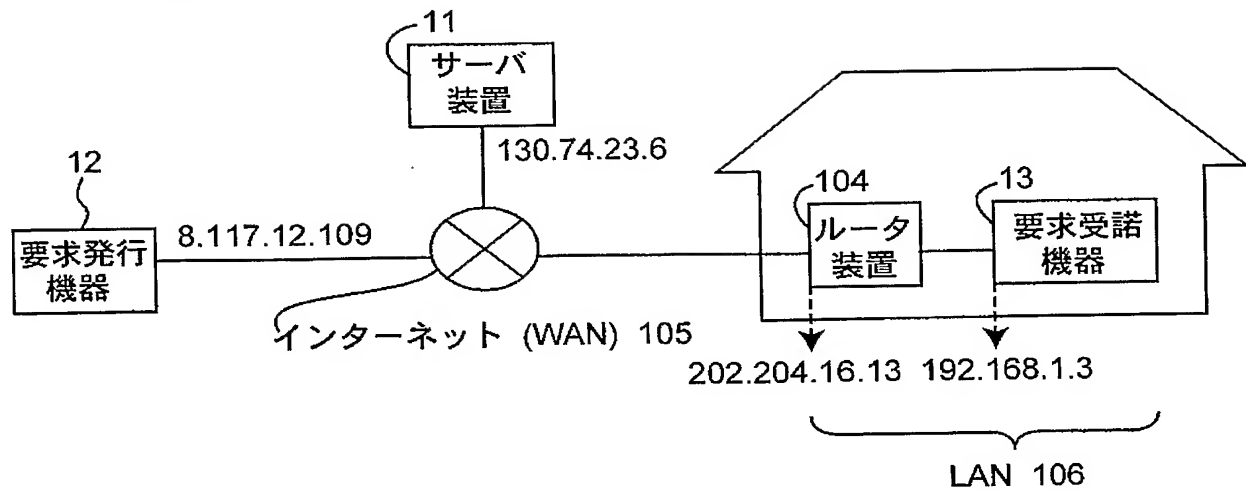
SA: 発信元アドレスフィールド、DA:宛先アドレスフィールド
 SP:発信元ポート番号フィールド、DP:宛先ポート番号フィールド

【図 9】

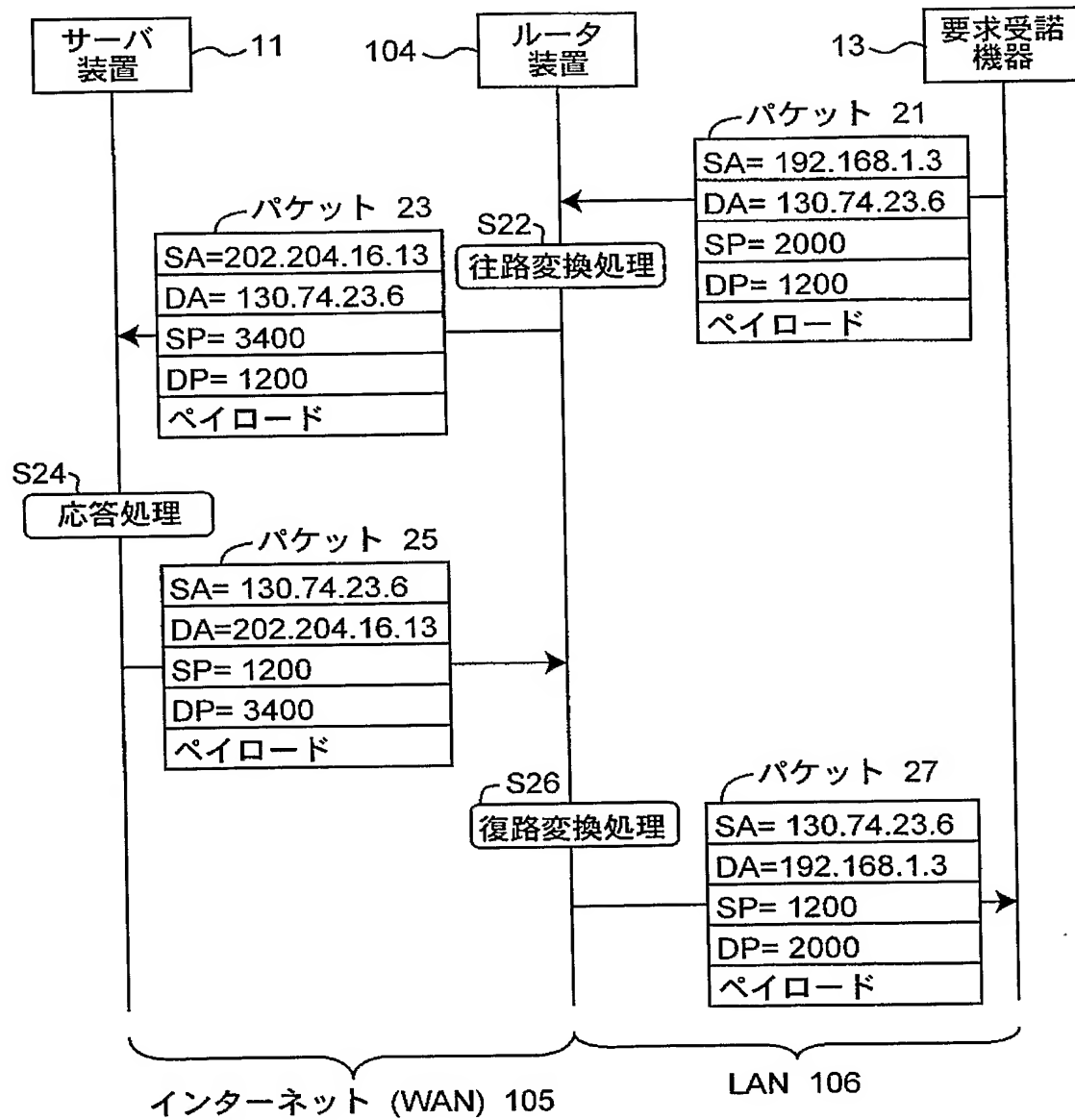
機器ID	IPアドレス	ポート番号
2133	202.204.16.13	3400
---	---	---
---	---	---

【図 10】

従来技術



【図 11】



【図 12】

LAN 機器アドレス	WAN ルータアドレス	LAN 機器ポート番号	WAN ルータポート番号
192.168.1.3	202.204.16.13	2000	3400
---	---	---	---
---	---	---	---

【書類名】要約書

【要約】

【課題】 プライベート IP アドレスを持つ異なる LAN 上の機器間でピアツーピア伝送を実現し不正アクセスを許さない。

【解決手段】 サーバ装置は、要求発行機器から送信される TCP 接続開始信号を受信して要求発行機器との間の TCP 接続を確立し、要求受諾機器の機器 ID と、要求発行機器の IP アドレス及びポート番号とを含む要求受諾機器への接続要求信号を要求発行機器から受信し、受信された接続要求信号に含まれる要求受諾機器の機器 ID を機器情報リストから検索し、接続要求信号に含まれる要求受諾機器の機器 ID と一致した機器 ID を含む機器情報の組に係る機器を要求受諾機器として識別し、これに係る機器情報の組に含まれる IP アドレス及びポート番号を要求受諾機器の IP アドレス及びポート番号として識別し、受信された接続要求信号に含まれる要求発行機器の IP アドレス及びポート番号を含む第 2 の接続要求信号を応答信号として送信する。

【選択図】 図 2

特願 2 0 0 4 - 0 4 4 1 4 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社